HCMUTE

CHƯƠNG I
TỔNG QUAN VỀ MẠNG MÁY TÍNH

GV. Nguyễn Thị Thanh Vân

Nội dung

- **Giới thiệu mạng và các loại mạng**
- **Mô hình OSI**
- **Mô hình TCP/IP**
- **Quá trình trao đổi dữ liệu qua mạng**
- **Các thành phần của gói dữ liệu mạng**

Quá trình trao đổi dữ liệu qua mạng

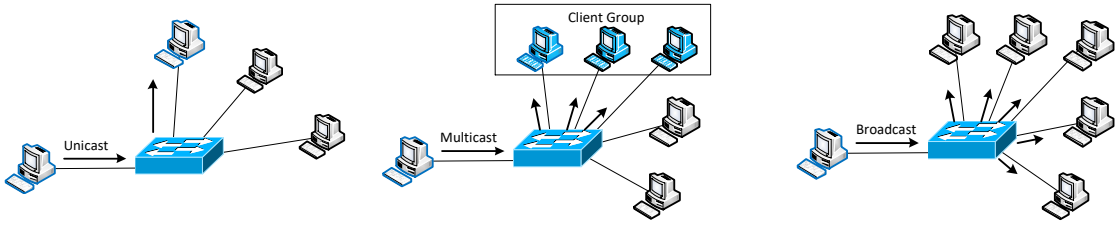
Nội dung

- Giới thiệu
- Đóng gói và mở gói dữ liệu
- Địa chỉ gói tin
- Hoạt động của ARP
- Phân tích gói tin ARP
- Khảo sát quá trình truyền dữ liệu qua
  - Hub hoặc trực tiếp
  - Switch
  - Router
- Thành phần gói tin

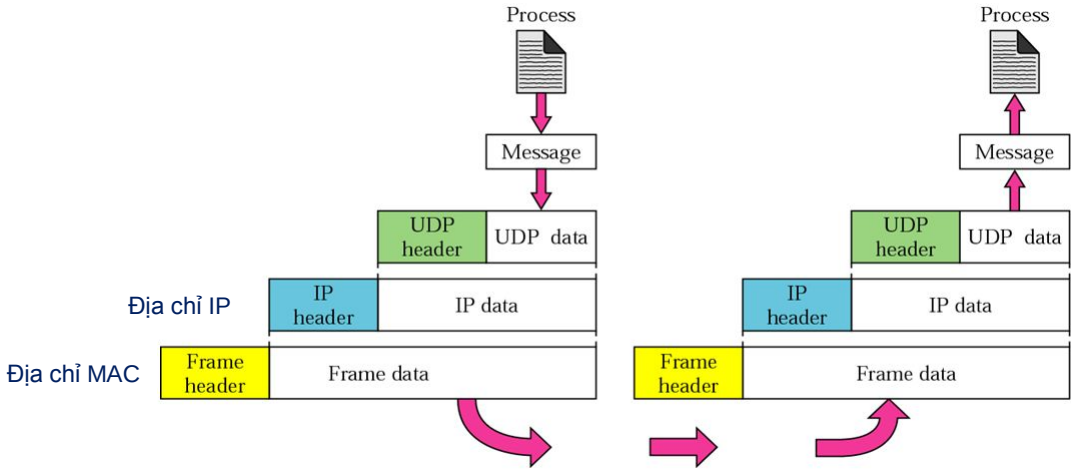
Giới thiệu

- Hai hoạt động chính trong truyền dữ liệu trên mạng:
  - Quá trình đóng gói bên máy gửi và mở gói bên máy nhận,
  - Quá trình truyền dữ liệu giữa hai máy qua mạng.
- Các kiểu truyền dữ liệu qua các thiết bị mạng gồm:

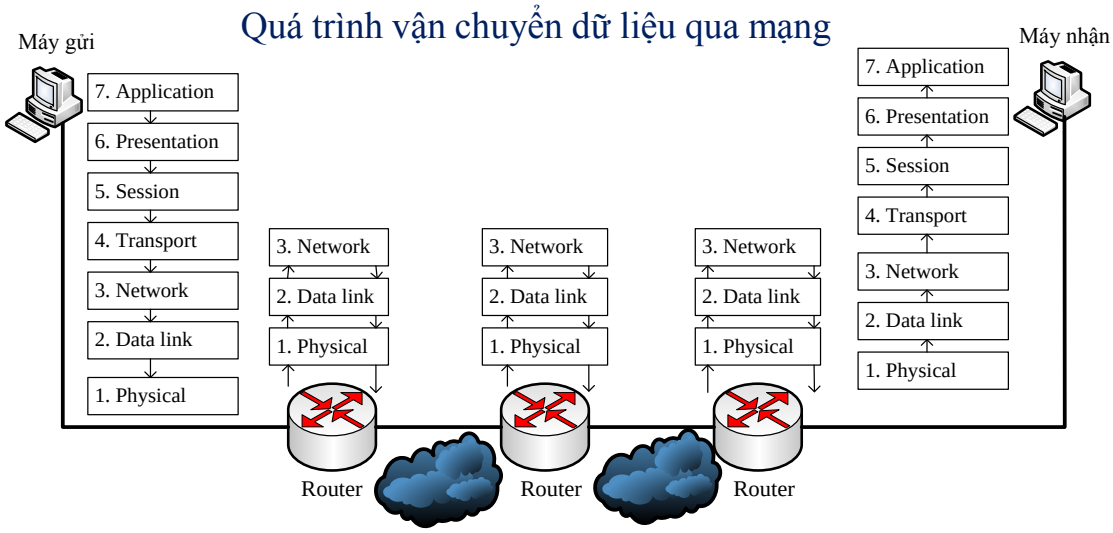
Unicast **Multicast** **Broadcast**



Đóng/mở gói dữ liệu theo TCP/IP

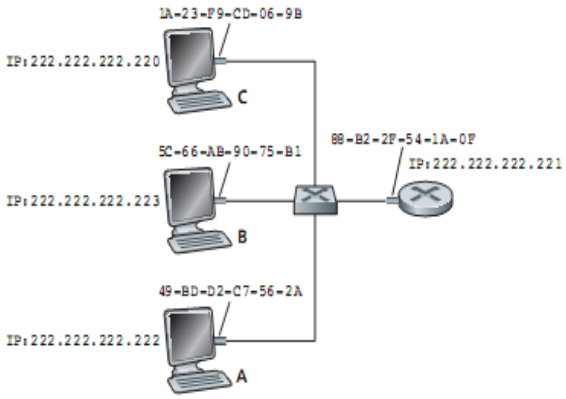


Đóng/mở gói dữ liệu theo TCP/IP



Địa chỉ của gói tin

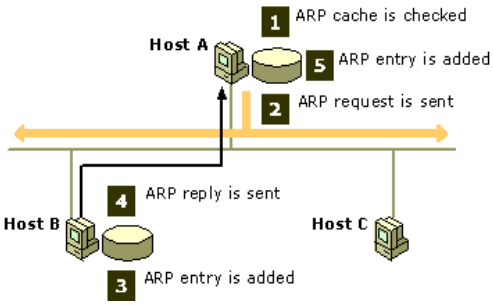
- Địa chỉ IP (Tầng Network)
  - Các giao tiếp mạng trên thiết bị đều có IP
  - Kích thước 32bit
- Địa chỉ MAC – Media Access Control (Tầng Datalink)
  - Được chỉ định bởi nhà sản xuất và được lưu trữ trong phần cứng các thiết bị như: card mạng của máy tính, cổng Router
  - Các giao tiếp mạng trên thiết bị đều có MAC
  - Kích thước 48byte – dạng hexadecimal

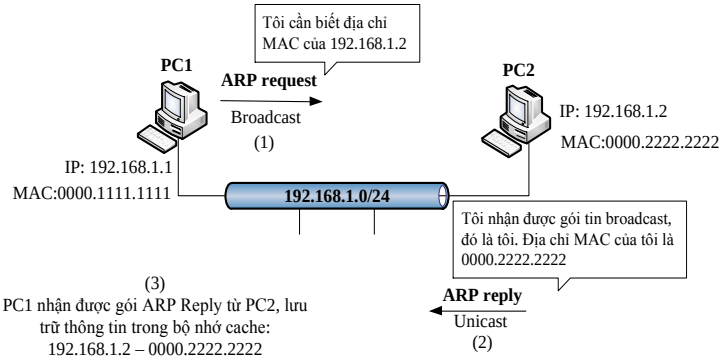


- Thiết bị ở tầng Link ko thể hiểu IP để chuyển packet đi, cần chuyển thành 1 địa chỉ MAC

Hoạt động của ARP

- Giao thức ARP – Address Resolution Protocol
  - ánh xạ địa chỉ MAC của một thiết bị khi biết IP của nó trong một miền quảng bá
  - Khi địa chỉ MAC đích chưa xác định được, máy tính sẽ dùng giao thức ARP để xác định giá trị này

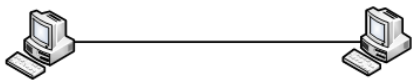




(3)
PC1 nhận được gói ARP Reply từ PC2, lưu trữ thông tin trong bộ nhớ cache:
192.168.1.2 – 0000.2222.2222

Phân tích gói dữ liệu ARP

- Dùng phần mềm Wireshark để bắt gói tin mạng



IP: 192.168.1.100
MAC: 9c:d2:1e:95:13:75

IP: 192.168.1.1
MAC: c8:3a:35:11:f0:40

ARP Request

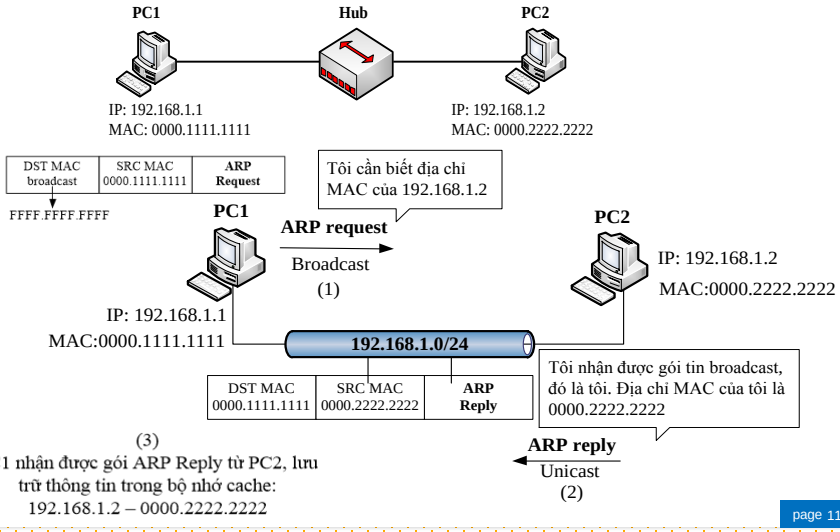
```
> Frame 2: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface 0
v Ethernet II, Src: HonHaiPr_95:13:75 (9c:d2:1e:95:13:75), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
  > Destination: Broadcast (ff:ff:ff:ff:ff:ff)
  > Source: HonHaiPr_95:13:75 (9c:d2:1e:95:13:75)
    Type: ARP (0x0806)
v Address Resolution Protocol (request)
    Hardware type: Ethernet (1)
    Protocol type: IPv4 (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: request (1)
    Sender MAC address: HonHaiPr_95:13:75 (9c:d2:1e:95:13:75)
    Sender IP address: 192.168.1.100
    Target MAC address: 00:00:00_00:00:00 (00:00:00:00:00:00)
    Target IP address: 192.168.1.1
```

ARP Reply

```
> Frame 3: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface 0
v Ethernet II, Src: TendaTec_11:f0:40 (c8:3a:35:11:f0:40), Dst: HonHaiPr_95:13:75 (9c:d2:1e:95:13:75)
  > Destination: HonHaiPr_95:13:75 (9c:d2:1e:95:13:75)
  > Source: TendaTec_11:f0:40 (c8:3a:35:11:f0:40)
    Type: ARP (0x0806)
v Address Resolution Protocol (reply)
    Hardware type: Ethernet (1)
    Protocol type: IPv4 (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: reply (2)
    Sender MAC address: TendaTec_11:f0:40 (c8:3a:35:11:f0:40)
    Sender IP address: 192.168.1.1
    Target MAC address: HonHaiPr_95:13:75 (9c:d2:1e:95:13:75)
    Target IP address: 192.168.1.100
```

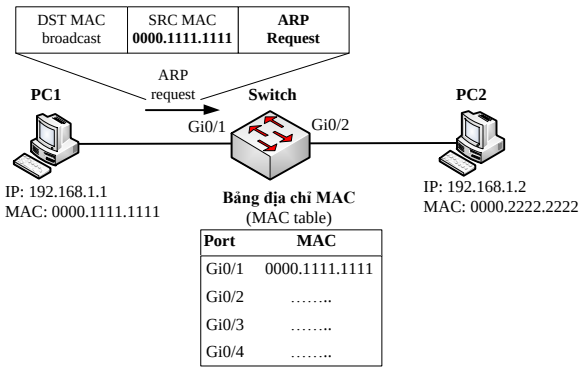
Khảo sát quá trình truyền dữ liệu qua Hub

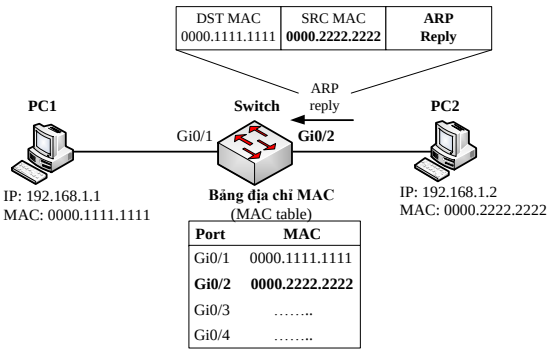
- Hai PC đều thuộc cùng một miền broadcast
- Thiết bị Hub ở tầng Physical
  - Nhận gói tin và gửi ra tất cả các port của nó nên các PC đều nhận được frame
- Các PC có cache:
  - lưu địa chỉ MAC của các máy giao tiếp với nó



Khảo sát quá trình truyền dữ liệu qua Switch

- Thiết bị Switch ở tầng Datalink.
- Switch có bảng MAC để ánh xạ switchport và địa chỉ MAC

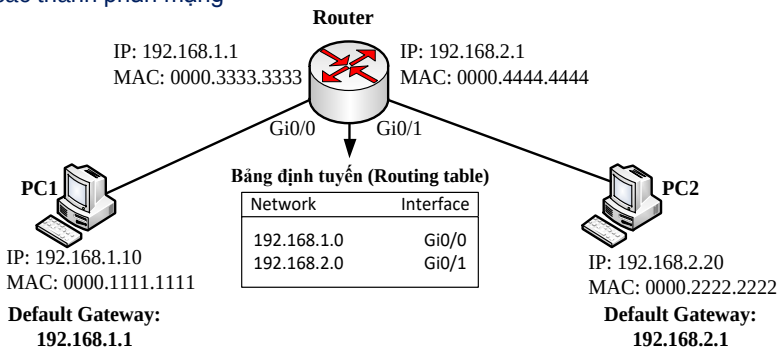




Khảo sát quá trình truyền dữ liệu qua Router

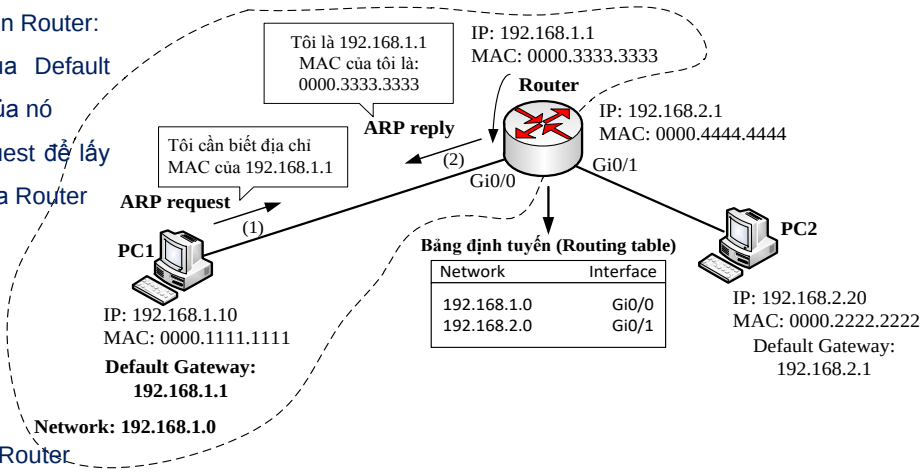
- Thiết bị Router ở tầng Network: Cần có bảng định tuyến để ánh xạ địa chỉ IP với Interface
- Các thông tin địa chỉ IP và MAC của các thành phần mạng
  - Router, tại 2 interface: IP, MAC
  - PC1: MAC, IP, Defaul Gateway
  - PC2: MAC, IP, Defaul Gateway

  (2 PC ở khác miền broadcast)
- Hoạt động: PC1 k/n với PC2
  - PC1 ko thể dùng ARP Request để tìm MAC của PC2.
  - Do: Router là thiết bị ngăn các tín hiệu broadcast



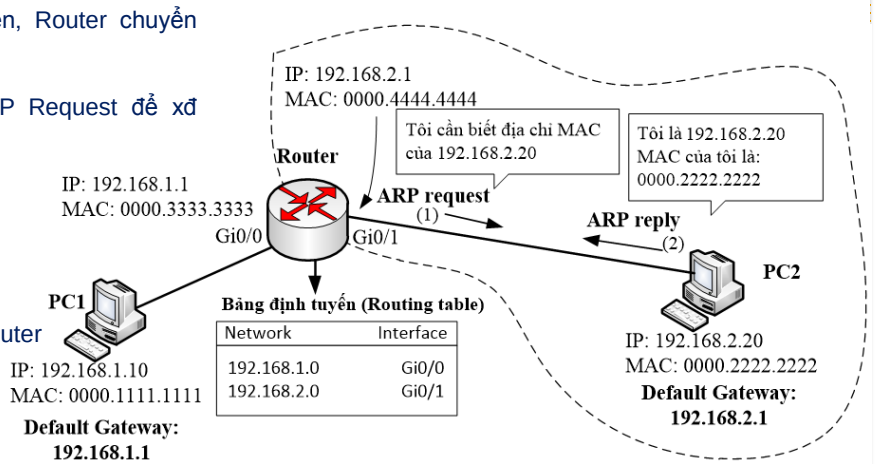
Khảo sát quá trình truyền dữ liệu qua Router

- Xét đoạn mạng từ PC1 đến Router:
  - PC1 sẽ k/tra IP của Default Gateway trong NIC của nó
  - PC1 dùng ARP Request để lấy địa chỉ MAC Gi0/0 của Router
- Kết quả:
  - IP nguồn: PC1
  - IP đích: PC2
  - MAC nguồn: PC1
  - MAC đích: Gi0/0 của Router



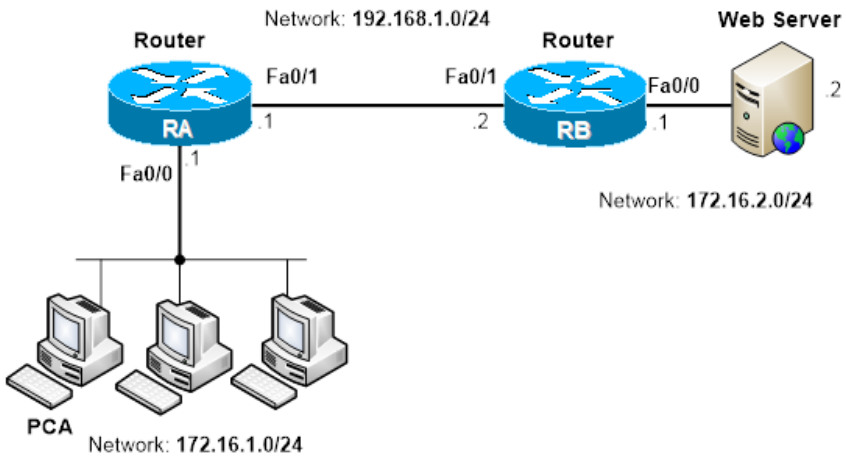
Khảo sát quá trình truyền dữ liệu qua Router

- Xét đoạn mạng từ Router đến PC2
  - Dựa vào bảng định tuyến, Router chuyển tiếp gói tin qua Gi0/1.
  - Tại layer2: Nó dùng ARP Request để xđ MAC đích
- Kết quả:
  - IP nguồn: PC1
  - IP đích: PC2
  - MAC nguồn: Gi0/1 của Router
  - MAC đích: PC2



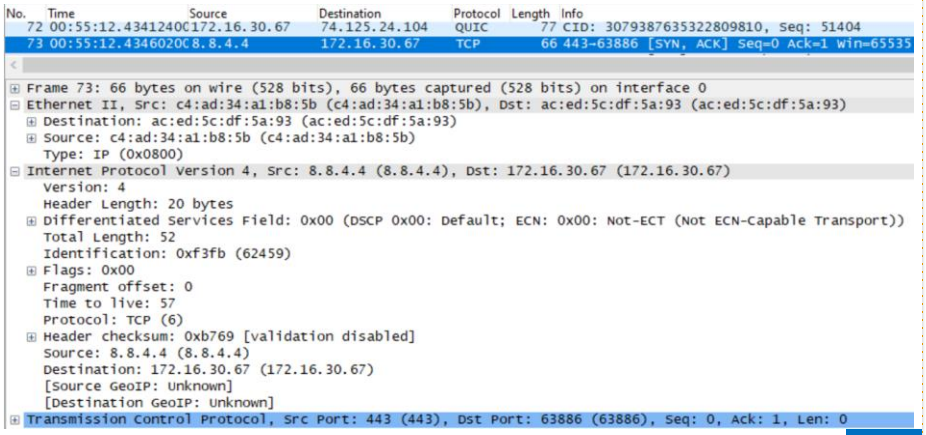
Ex

Xác định thông tin gói tin đi qua từng đoạn mạng khác nhau



Các thành phần gói tin

- Phân tích thành phần gói tin mạng dùng phần mềm bắt gói - Wireshark
- Gói tin gồm: các phần
  - Frame
  - Ethernet II
  - IP v4
  - TCP



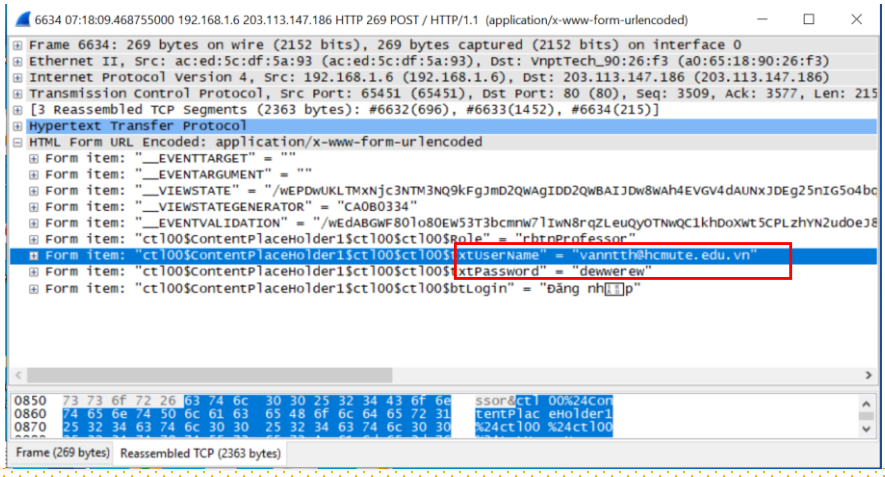
Thực hành

- Dùng Wireshark để bắt gói dữ liệu mạng bình thường
  - Truy cập các dịch vụ khác nhau trên mạng như: web, email, chuyển nhận file, message
  - Bắt gói tin và phân tích
- Bắt gói dữ liệu tấn công mạng

Thực hành

Dùng Wireshark để bắt gói dữ liệu mạng

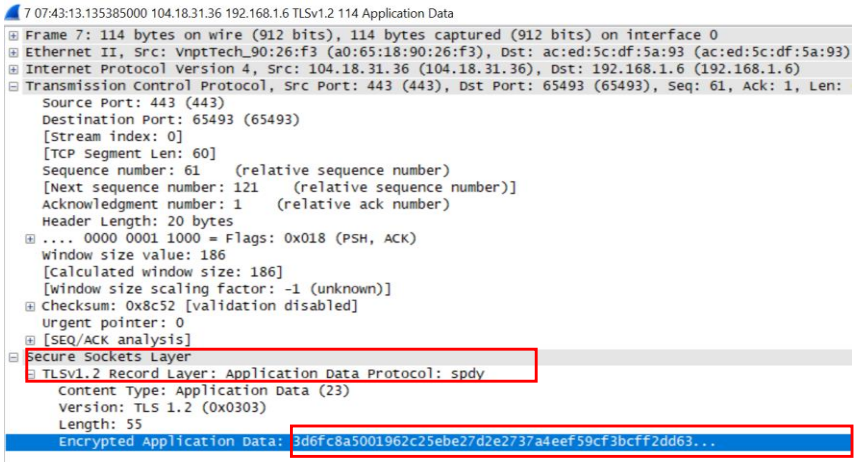
- Bắt gói tin http khi thao tác đăng nhập usename/password: đọc được



Thực hành

Dùng Wireshark để bắt gói dữ liệu mạng

- Bắt gói tin https khi thao tác đăng nhập usename/password: đã mã hóa



Bài tập thực hành

- Dùng Wireshark để bắt gói dữ liệu mạng khi truy cập một số trang web (http và https)có yêu cầu xác thực
  - http://elearning.tbump.edu.vn/
  - https bất kì
- Chụp kết quả của nội dung gói tin bắt được và phân tích
- Câu hỏi:
  - Nội dung gói tin khi truy cập trang web có giao thức http và https có gì khác nhau
- Nộp bài theo lịch thông báo

HCMUTE

Kết thúc Chương 1