



1



HCMUTE



2

# 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**

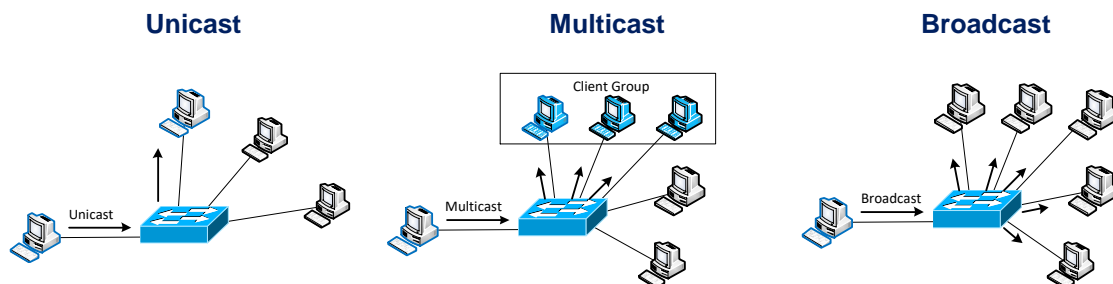
# Quá trình trao đổi dữ liệu qua mạng

## 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

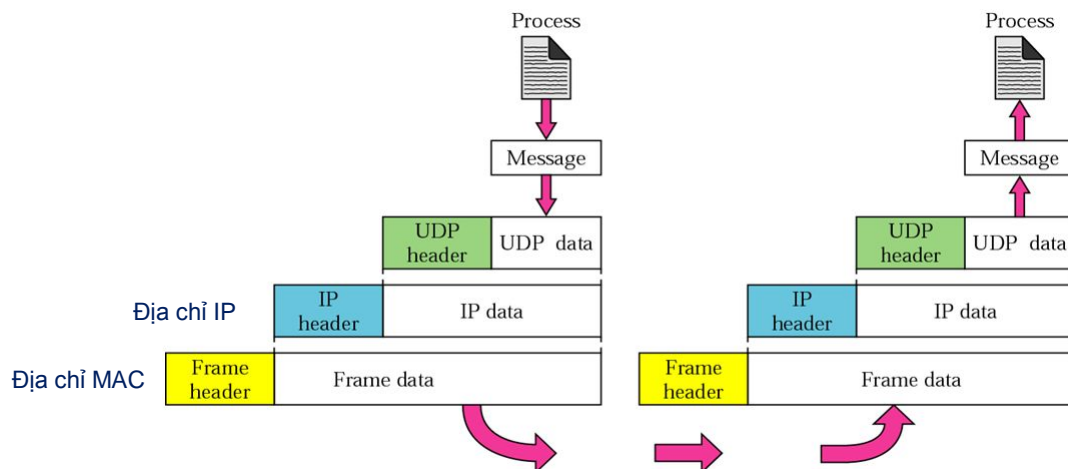
## Giới thiệu

- ❖ 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:



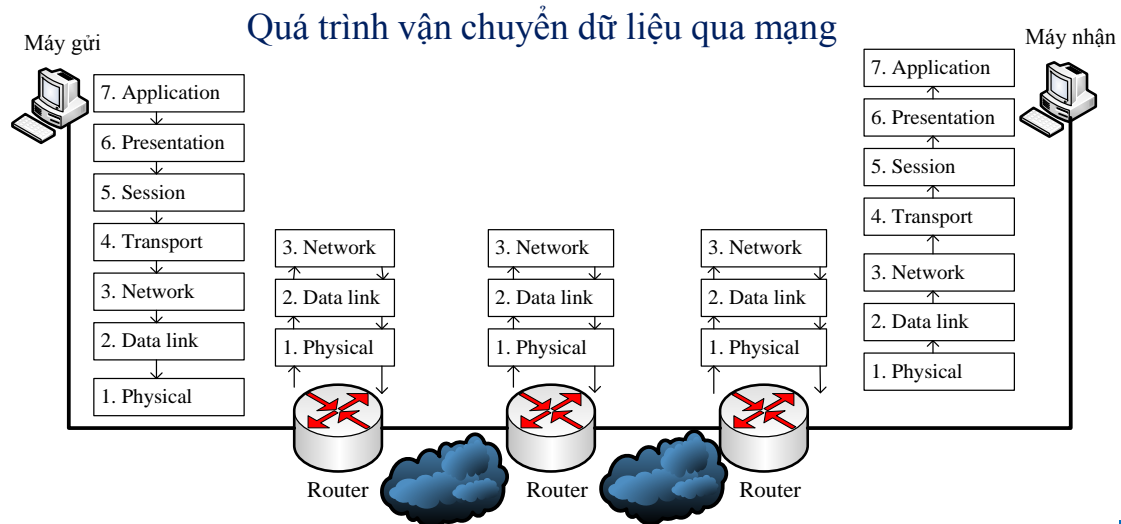
page 5

## Đóng/mở gói dữ liệu theo TCP/IP



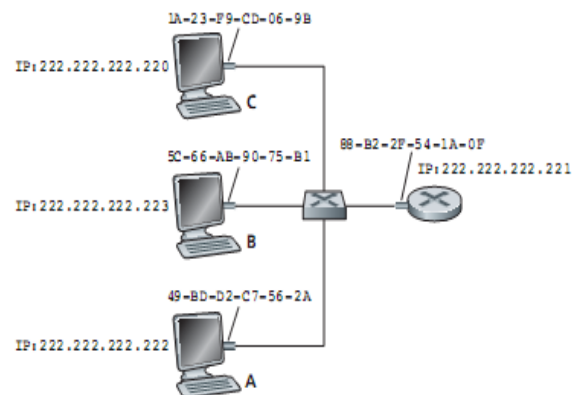
page 6

# Đóng/mở gói dữ liệu theo TCP/IP



## Địa chỉ của gói tin

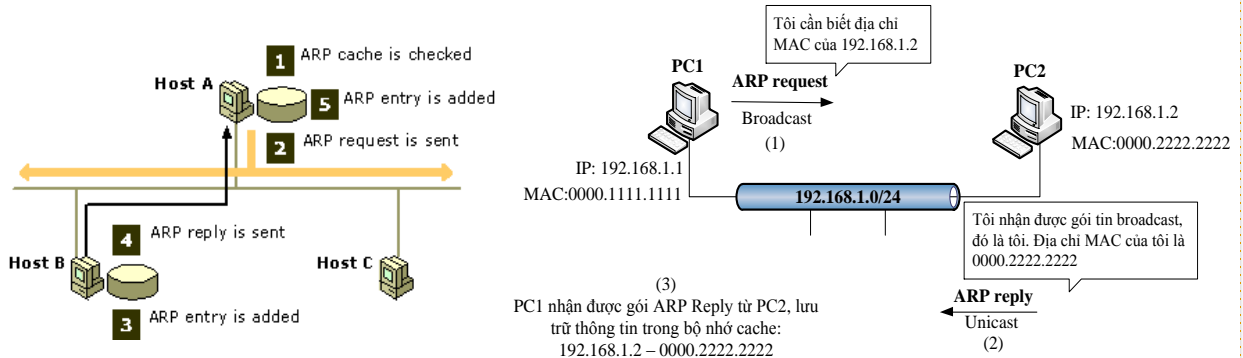
- ❖ Địa chỉ IP (Tầng Network)
  - ❖ Các giao tiếp mạng trên thiết bị đều có IP
  - ❖ Kích thước 32bit
- ❖ Địa chỉ MAC – Media Access Control (Tầng Datalink)
  - ❖ Được chỉ định bởi nhà sản xuất và được lưu trữ trong phần cứng các thiết bị như: card mạng của máy tính, cổng Router
  - ❖ Các giao tiếp mạng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

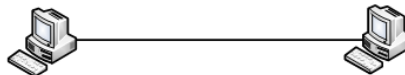
- ❖ ánh xạ địa chỉ MAC của một thiết bị khi biết IP của nó trong một miền quảng bá
- ❖ Khi địa chỉ MAC đích chưa xác định được, máy tính sẽ dùng giao thức ARP để xác định giá trị này



page 9

# 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

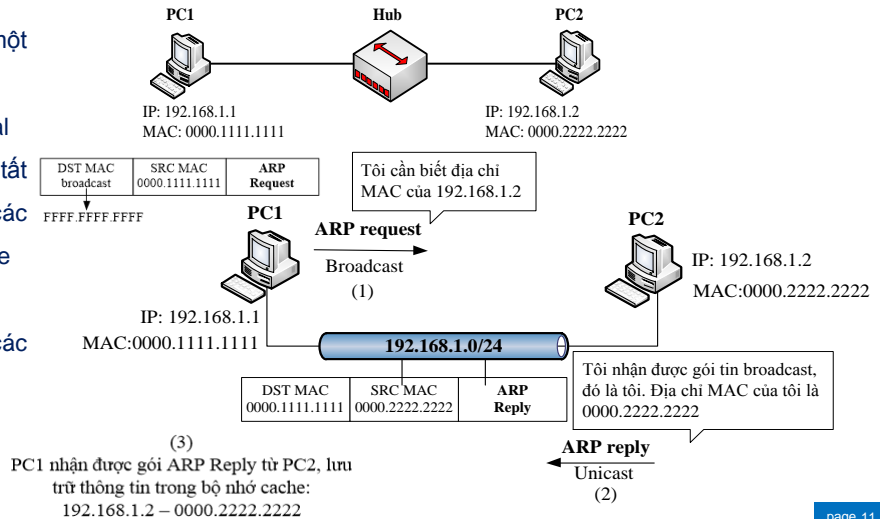
```
> Frame 2: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface 0
> Ethernet II, Src: HonHaiPr_95:13:75 (9c:d2:1e:95:13:75), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
  > Destination: Broadcast (ff:ff:ff:ff:ff:ff)
  > Source: HonHaiPr_95:13:75 (9c:d2:1e:95:13:75)
    Type: ARP (0x0806)
  > 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
> 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)
  > 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

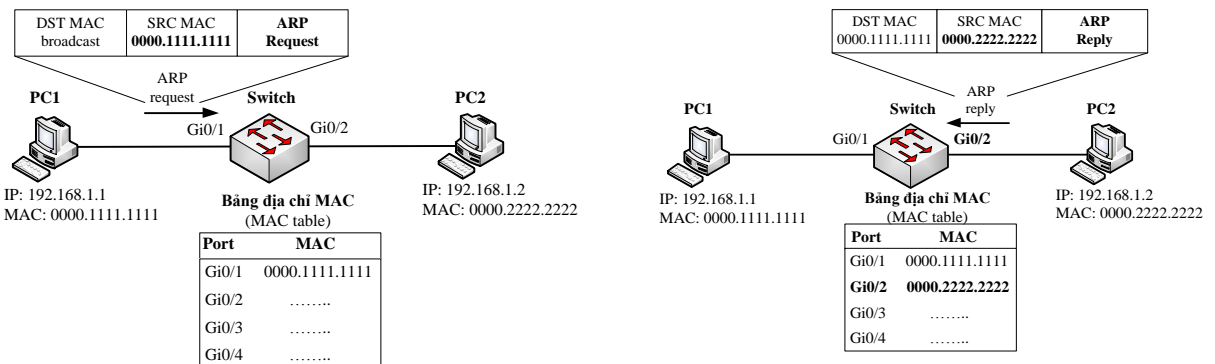
- ❖ Hai PC đều thuộc cùng một miền broadcast
- ❖ Thiết bị Hub ở tầng Physical
- ❖ Nhận gói tin và gửi ra tất cả các port của nó nên các PC đều nhận được frame
- ❖ Các PC có cache:
  - ❖ lưu địa chỉ MAC của các máy giao tiếp với nó



page 11

## 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



page 12

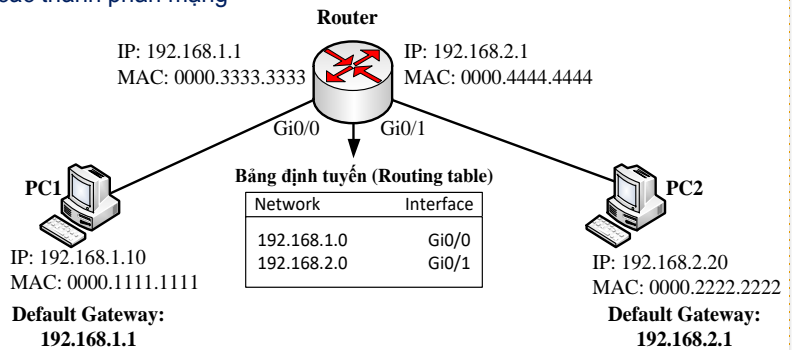
## Khảo sát quá trình truyền dữ liệu qua Router

- ❖ 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, Default Gateway
- ❖ PC2: MAC, IP, Default 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



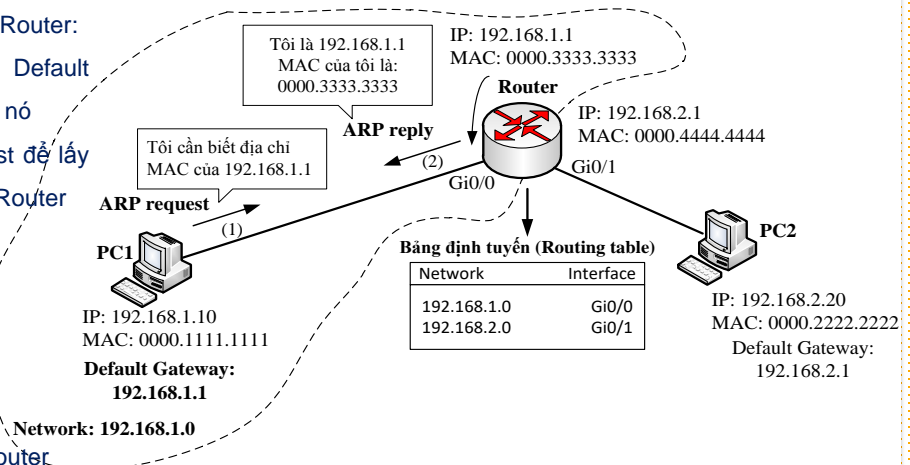
page 13

## 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



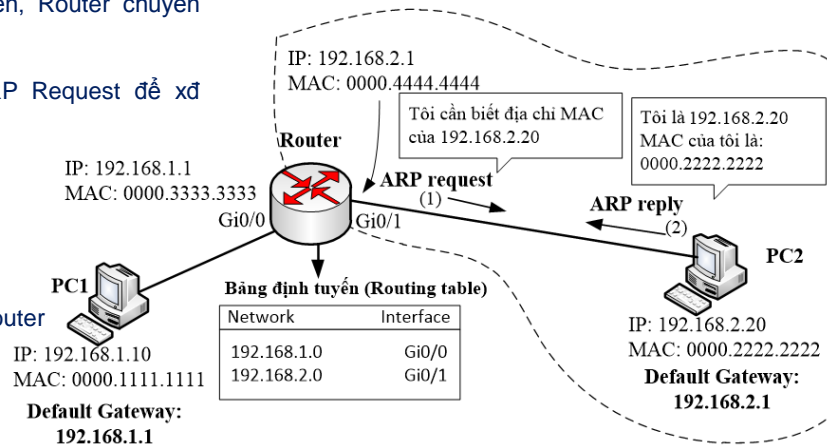
page 14

## 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:

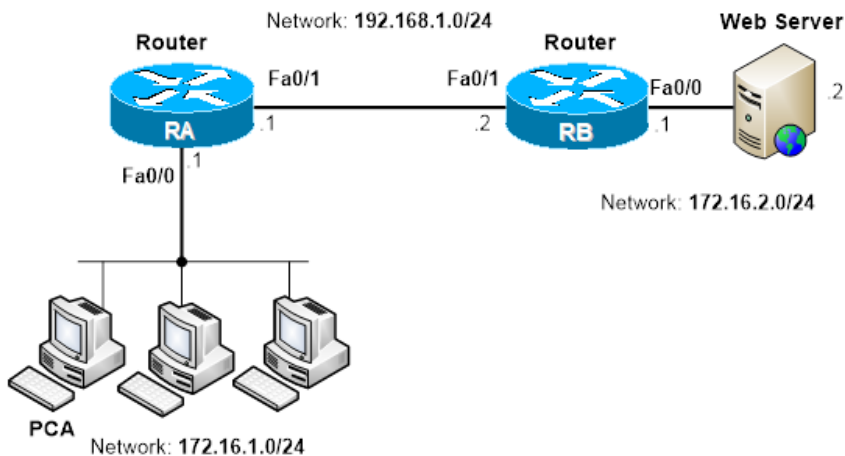
- ❖ IP nguồn: PC1
- ❖ IP đích: PC2
- ❖ MAC nguồn: Gi0/1 của Router
- ❖ MAC đích: PC2



page 15

## Ex

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



page 16



# 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

No.	Time	Source	Destination	Protocol	Length	Info
72	00:55:12.4341240	172.16.30.67	74.125.24.104	QUIC	77	CID: 3079387635322809810, Seq: 51404
73	00:55:12.4346020	8.8.4.4	172.16.30.67	TCP	66	443→63886 [SYN, ACK] Seq=0 Ack=1 Win=65535
<						
<ul style="list-style-type: none"> <li>Frame 73: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface 0</li> <li>Ethernet II, Src: c4:ad:34:a1:b8:5b (c4:ad:34:a1:b8:5b), Dst: ac:ed:5c:df:5a:93 (ac:ed:5c:df:5a:93) <ul style="list-style-type: none"> <li>Destination: ac:ed:5c:df:5a:93 (ac:ed:5c:df:5a:93)</li> <li>Source: c4:ad:34:a1:b8:5b (c4:ad:34:a1:b8:5b)</li> <li>Type: IP (0x0800)</li> </ul> </li> <li>Internet Protocol Version 4, Src: 8.8.4.4 (8.8.4.4), Dst: 172.16.30.67 (172.16.30.67) <ul style="list-style-type: none"> <li>Version: 4</li> <li>Header Length: 20 bytes</li> <li>Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00: Not-ECT (Not ECN-Capable Transport))</li> <li>Total Length: 52</li> <li>Identification: 0xf3fb (62459)</li> <li>Flags: 0x00</li> <li>Fragment offset: 0</li> <li>Time to live: 57</li> <li>Protocol: TCP (6)</li> <li>Header checksum: 0xb769 [validation disabled]</li> <li>Source: 8.8.4.4 (8.8.4.4)</li> <li>Destination: 172.16.30.67 (172.16.30.67)</li> <li>[Source GeoIP: Unknown]</li> <li>[Destination GeoIP: Unknown]</li> </ul> </li> <li>Transmission Control Protocol, Src Port: 443 (443), Dst Port: 63886 (63886), Seq: 0, Ack: 1, Len: 0</li> </ul>						

page 17

# 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

page 18

# Thực hành

Dùng Wireshark để bắt gói dữ liệu mạng

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

```

6634 07:18:09.468755000 192.168.1.6 203.113.147.186 HTTP 269 POST / HTTP/1.1 (application/x-www-form-urlencoded)
  Frame 6634: 269 bytes on wire (2152 bits), 269 bytes captured (2152 bits) on interface 0
  Ethernet II, Src: ac:ed:5c:df:5a:93 (ac:ed:5c:df:5a:93), Dst: vnptech_90:26:f3 (a0:65:18:90:26:f3)
  Internet Protocol Version 4, Src: 192.168.1.6 (192.168.1.6), Dst: 203.113.147.186 (203.113.147.186)
  Transmission Control Protocol, Src Port: 65451 (65451), Dst Port: 80 (80), Seq: 3509, Ack: 3577, Len: 215
  [3 Reassembled TCP Segments (2363 bytes): #6632(696), #6633(1452), #6634(215)]
  Hypertext Transfer Protocol
    HTML Form URL Encoded: application/x-www-form-urlencoded
    Form item: "_EVENTTARGET" = ""
    Form item: "_EVENTARGUMENT" = ""
    Form item: "_VIEWSTATE" = "/wEPDwUKLTmXNjc3NTM3NQ9kFgJmD2QWAgIDD2QWBAIJDw8WAH4EVGV4dAUNXJDEg25nIG504bc"
    Form item: "_VIEWSTATEGENERATOR" = "CA0B0334"
    Form item: "_EVENTVALIDATION" = "/wEABGWF801o80EW53T3bcmw71Iwn8rqZLeuqyOTNwQC1khd0xwt5CPLzhYN2udoe38"
    Form item: "ctl00$ContentPlaceHolder1$ctl00$ctl00$Role" = "chinaProfessor"
    Form item: "ctl00$ContentPlaceHolder1$ctl00$ctl00$xtUserName" = "vaninthanhcmute.edu.vn"
    Form item: "ctl00$ContentPlaceHolder1$ctl00$ctl00$xtPassword" = "dewierew"
    Form item: "ctl00$ContentPlaceHolder1$ctl00$ctl00$btLogin" = "Đăng nh[...]"
  
```

page 19

# Thực hành

Dùng Wireshark để bắt gói dữ liệu mạng

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

```

7 07:43:13.135385000 104.18.31.36 192.168.1.6 TLSv1.2 114 Application Data
  Frame 7: 114 bytes on wire (912 bits), 114 bytes captured (912 bits) on interface 0
  Ethernet II, Src: vnptech_90:26:f3 (a0:65:18:90:26:f3), Dst: ac:ed:5c:df:5a:93 (ac:ed:5c:df:5a:93)
  Internet Protocol Version 4, Src: 104.18.31.36 (104.18.31.36), Dst: 192.168.1.6 (192.168.1.6)
  Transmission Control Protocol, Src Port: 443 (443), Dst Port: 65493 (65493), Seq: 61, Ack: 1, Len:
    Source Port: 443 (443)
    Destination Port: 65493 (65493)
    [Stream index: 0]
    [TCP Segment Len: 60]
    Sequence number: 61 (relative sequence number)
    [Next sequence number: 121 (relative sequence number)]
    Acknowledgment number: 1 (relative ack number)
    Header Length: 20 bytes
    .... 0000 0001 1000 = Flags: 0x018 (PSH, ACK)
    window size value: 186
    [calculated window size: 186]
    [window size scaling factor: -1 (unknown)]
    Checksum: 0x8c52 [validation disabled]
    urgent pointer: 0
    [SEQ/ACK analysis]
  Secure Sockets Layer
    TLSv1.2 Record Layer: Application Data Protocol: spdy
    Content Type: Application Data (23)
    Version: TLS 1.2 (0x0303)
    Length: 55
    Encrypted Application Data: 3d6fc8a5001962c25ebe27d2e2737a4eef59cf3bcff2dd63...
  
```

page 20

## 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



## Kết thúc Chương 1