BÁO CÁO THỰC HÀNH

**Bài thực hành số 01: Tìm hiểu WLAN 802.11**

**GVHD: Nguyễn Khánh Thuật**

**Môn học:** Hệ Thống Nhúng & Mạng Không Dây

**Lớp:** NT131.O12.MMCL

**THÀNH VIÊN THỰC HIỆN:**

|  |  |  |
| --- | --- | --- |
| **STT** | **Họ và tên** | **MSSV** |
| 1 | Ngô Thế Anh | 21521826 |
| 2 | Lê Hoàng Khánh | 21521826 |

|  |
| --- |
| **Điểm tự đánh giá** |
| **9.5** |

**ĐÁNH GIÁ KHÁC:**

|  |  |
| --- | --- |
| Tổng thời gian thực hiện | 2 Tuần |
| Phân chia công việc | - Thế Anh: Tìm hiểu file PCAP, Viết báo cáo, Capture thực tế.  - Hoàng Khánh: Tìm hiểu và chạy NS-3, Lên nội dụng báo cáo, Hiệu chỉnh báo cáo. |
| Ý kiến *(nếu có)*  + Khó khăn  + Đề xuất, kiến nghị |  |

MỤC LỤC

[**A.** BÁO CÁO CHI TIẾT 4](#_Toc147952397)

[1. Tìm hiểu nội dung code được cung cấp, trình bày ý tưởng kịch bản, các bước cài đặt trong code để xây dựng nên kịch bản 4](#_Toc147952398)

[a. Giới thiệu. 4](#_Toc147952399)

[b. Nội dung. 4](#_Toc147952400)

[c. Ý tưởng. 4](#_Toc147952401)

[d. Các bước cài đặt để xây dựng kịch bản trên. 5](#_Toc147952402)

[e. Chạy đoạn code qua ns3. 7](#_Toc147952403)

[2. Tìm hiểu, trình bày và thực hiện log ra 3 file .pcap của 3 node: UDP Client, UDP Server và AP. 8](#_Toc147952404)

[a. Chỉnh sửa code để thực hiện yêu cầu. 8](#_Toc147952405)

[b. Chạy lại chương trình trên. 8](#_Toc147952406)

[3. Các Beacon frames là gì? có ý nghĩa như thế nào? Giải thích. Tìm trên các Beacon frames, SSID của AP là gì? 9](#_Toc147952407)

[4. Tìm các gói tin thể hiện quá trình kết nối giữa các node và AP. Các thông điệp này có ý nghĩa gì? 10](#_Toc147952408)

[5. Tìm hiểu quá trình khởi tạo kết nối UDP và chỉ ra các gói tin UDP đi từ client đến server và ngược lại. Giải thích sự tương quan giữa code và file .pcap. 11](#_Toc147952409)

[a. Quá trình khởi tạo kết nối UDP 11](#_Toc147952410)

[b. Tương quan giữa code và file .pcap.  15](#_Toc147952411)

[6. Khoảng thời gian giữa các lần truyền Beacon frames là bao nhiêu? Hãy chứng minh điều đó. 16](#_Toc147952412)

[7. Địa chỉ MAC nguồn, đích, BSSID trong 802.11 frame có giá trị bao nhiêu (dưới dạng thập lục phân)? Chúng có ý nghĩa như thế nào và chiếm bao nhiêu bytes trong cấu trúc gói tin? 17](#_Toc147952413)

[8. Trong các Beacon frames quảng bá rằng có thể hỗ trợ nhiều data rates khác nhau, tìm các thông tin này? Cho biết các rates này có ý nghĩa gì? 18](#_Toc147952414)

[9. Có tổng cộng bao nhiêu AP xung quanh, SSID của các AP này là gì? Hãy chứng minh điều đó. 19](#_Toc147952415)

[10. Thực hiện lại các câu hỏi 6, 7, 8. Các trường / nội dung này có gì đặt biệt, khác nhau giữa 2 kịch bản. 20](#_Toc147952416)

[a. Khoảng thời gian giữa các lần truyền Beacon frames là bao nhiêu? Hãy chứng minh điều đó. 20](#_Toc147952417)

[b. Địa chỉ MAC nguồn, đích, BSSID trong 802.11 frame có giá trị bao nhiêu (dưới dạng thập lục phân)? Chúng có ý nghĩa như thế nào và chiếm bao nhiêu bytes trong cấu trúc gói tin? 21](#_Toc147952418)

[c. Trong các Beacon frames quảng bá rằng có thể hỗ trợ nhiều data rates khác nhau, tìm các thông tin này? Cho biết các rates này có ý nghĩa gì? 22](#_Toc147952419)

[11. Tìm các gói tin Probe Request và Probe Response trong các 802.11 frames. Mục đích của các gói tin này dùng để làm gì? Địa chỉ MAC nguồn, đích, BSSID của chúng như thế nào? 23](#_Toc147952420)

[a. Gói tin Probe Request 23](#_Toc147952421)

[b. Gói tin Prob Response 24](#_Toc147952422)

[12. Tìm cặp gói tin Authentication được gửi từ client đến AP và ngược lại, cho biết chúng dùng để làm gì? Các trường Authentication Algorithm, Authentication SEQ, Satatus code trong các gói tin Authentication ở trên thể hiện điều gì? 25](#_Toc147952423)

[a. Cặp gói tin Authentication. 25](#_Toc147952424)

[b. Các trường Authentication. 26](#_Toc147952425)

[13. Tìm các gói tin Association được gửi từ client và ngược lại, trường thông tin nào cho biết chúng là một Association Request hay một Association Response? Tìm các thông tin Capabilities Information, SSID, rates supported trong Association Request và cho biết chúng có ý nghĩa như thế nào? 28](#_Toc147952426)

[14. Giữa Association Request và Association Response có xuất hiện thêm trường gì đặt biệt? Giá trị của nó là bao nhiêu? 30](#_Toc147952427)

[15. Từ các nội dung đã tìm hiểu, trình bày quá trình WLAN 802.11 hoạt động thông qua các gói tin và sự khác nhau giữa kịch bản 1 và kịch bản 2. 31](#_Toc147952428)

[**B.** TÀI LIỆU THAM KHẢO 33](#_Toc147952429)

# BÁO CÁO CHI TIẾT

## Tìm hiểu nội dung code được cung cấp, trình bày ý tưởng kịch bản, các bước cài đặt trong code để xây dựng nên kịch bản

### Giới thiệu.

Đoạn code sử dụng NS-3 (Network Simulator 3) đây là một công cụ mô phỏng mạng mạnh mẽ, linh hoạt, mã nguồn mở, được phát triển bởi nhiều tổ chức và cá nhân trên thế giới. NS-3 có thể được sử dụng để mô phỏng một loạt các mạng và giao thức mạng khác nhau. NS-3 được sử dụng rộng rãi trong nghiên cứu và phát triển mạng, cũng như trong giáo dục.

### Nội dung.

Đoạn code trên được lập trình để mô phỏng kịch bản một mạng WiFi đơn giản bao gồm các thành phần:

* 5 node Wi-Fi Station
* 1 node Wi-Fi Access Point
* Kênh truyền dẫn Wi-Fi
* Mô hình di động ngẫu nhiên cho các Station

### Ý tưởng.

Ý tưởng kịch bản này được thực hiện theo các bước sau:

1. Tạo các Station và AP.
2. Thiết lập kênh truyền dẫn Wi-Fi.
3. Thiết lập mô hình di động ngẫu nhiên cho các Station.
4. Cài đặt giao thức TCP/IP và gán địa chỉ IP cho các node.
5. Cài đặt ứng dụng **UdpEchoServer** trên Station cuối cùng và ứng dụng **UdpEchoClient** trên Station thứ hai.
6. Khởi động các ứng dụng **UdpEchoClient** và **UdpEchoServer**.
7. Mô phỏng trong 10 giây.
8. Dừng mô phỏng.

### Các bước cài đặt để xây dựng kịch bản trên.

1. **Tạo các Station và AP**. Sử dụng **NodeContainer** để tạo các Station. Số lượng Station được chỉ định bởi tham số **nWifi**. Sử dụng Station thứ nhất làm AP.

A computer screen shot of a code

Description automatically generated

1. Cài đặt kênh và thiết bị wifi. Sử dụng **YansWifiChannel** và **YansWifiPhy** để thiết lập kênh, sử dụng kênh mặc định và lập trình lỗi mạng theo mô hình **NistErrorRateModel**. Thiết lập mô hình WiFi, SSID, quản lý trạm từ xa, và thiết lập kiểu MAC (MAC Type) cho các Station.

A computer screen with text

Description automatically generated

1. Thiết lập mô hình di động ngẫu nhiên cho các Station. Sử dụng **MobilityHelper** để tạo mô hình di động cho các Station. Các thông số như vị trí ban đầu, tốc độ và phạm vi di chuyển có thể xác định. Trong đoạn code trên, các station di chuyển theo mô hình **RandomWalk2dMobilityModel**, trong khi AP có vị trí cố định.

A screen shot of a computer program

Description automatically generated

1. Cài đặt giao thức TCP/IP và gán địa chỉ IP cho các Station. Sử dụng InternetStackHelper để cài đặt giao thức mạng Internet cho các nút WiFi. Thiết lập địa chỉ IP cho các Station và AP sử dụng **Ipv4AddressHelper**.

A screen shot of a computer program

Description automatically generated

1. Cài đặt **UdpEchoServer** trên Station cuối cùng **(wifiStaNodes.Get(nWifi - 1))** và ứng dụng **UDPEchoClient** chạy trên Station thứ thứ hai **(wifiStaNodes.Get(1))** (thứ nhất là AP)**.**

A screen shot of a computer program

Description automatically generated

1. Thiết lập bảng định tuyến. Sử dụng **Ipv4GlobalRoutingHelper** để tạo và cập nhật bảng định tuyến.



1. Chạy và kết thúc mô phỏng. Thiếp lập thời gian dừng mô phòng là sau 10 giây sau khi chạy. Sau đó dọn dẹp và kết thúc mô phỏng.

A screenshot of a computer program

Description automatically generated

### Chạy đoạn code qua ns3.

1. Để chạy được ns-3 ta cần phải cài các depency được yêu câu, chi tiết tại wiki của ns-3: <https://www.nsnam.org/wiki/Installation#Linux>
2. Tải ns3, phiên bản mới nhất hiện tại là 3.40 qua các câu lệnh sau.

$ cd

$ mkdir workspace

$ cd workspace

$ wget https://www.nsnam.org/release/ns-allinone-3.40.tar.bz2

$ tar xjf ns-allinone-3.40.tar.bz2  
$ cd ns-allinone-3.40/ns-3.40

1. Tại **ns-3.40** copy file **lab1-student.cc** vào folder **scratch.**
2. Configure và Build ns-3.

$ ./ns3 configure --enable-examples --enable-tests –enable-python-bindings

$ ./ns3 build

1. Sau khi đã build xong, để chạy **lab1-student.cc** ta thực hiện lệnh.

$ ./ns3 run scratch/lab1-student.cc -–vis

Ta cần thêm option --vis để hiện mô phỏng của kịch bản. Ta sẽ được giao diện như sau. Có 4 node là Station và 1 node là AP. Và 4 Station cùng kết nối đến cùng AP. Ấn **Simulate** để bắt đầu mô phỏng, ấn lần hai sẽ tạm dừng mô phỏng.

A screen shot of a computer

Description automatically generated

## Tìm hiểu, trình bày và thực hiện log ra 3 file .pcap của 3 node: UDP Client, UDP Server và AP.

### Chỉnh sửa code để thực hiện yêu cầu.

A screen shot of a computer

Description automatically generated

Để thực hiện xuất pcap ta sử dụng method **EnablePcap** với param thứ nhất là tên file, thứ hai là Device được lấy từ **apDevices** và **staDevices,** cuối cùng **true** giúp ta có thể bắt được gói tin UDP.

### Chạy lại chương trình trên.

Ta thực hiện update build bằng lệnh.

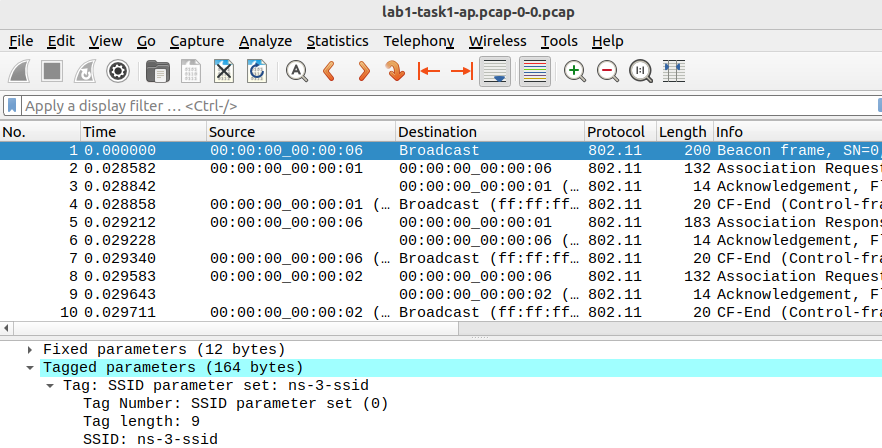
# ./ns3 build

Sau khi build xong ta thực hiện chạy chương trình như hướng dẫn ở trên. Ta sẽ được 3 file như yêu cầu của đề bài.

## Các Beacon frames là gì? có ý nghĩa như thế nào? Giải thích. Tìm trên các Beacon frames, SSID của AP là gì?

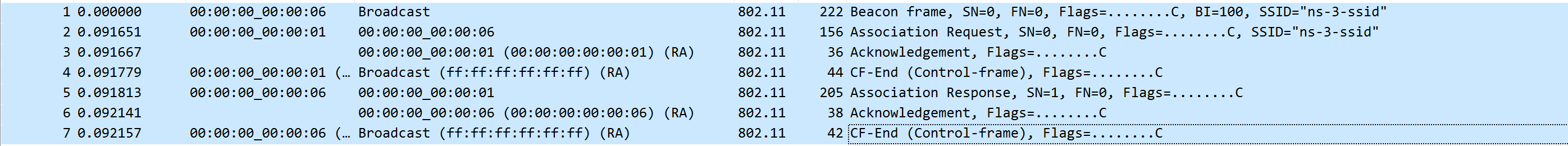
Các **Beacon frames** là khung thông tin được gửi từ **Access Point** (AP) trong mạng Wi-Fi đến các **Station**. Chúng chứa thông tin về tên mạng (**SSID**), địa chỉ AP (**BSSID**), thông số mạng, tần số hoạt động và thời gian sử dụng kênh. Các **Beacon frames** giúp thiết bị trạm tìm kiếm, xác định và kết nối đến AP phù hợp trong mạng Wi-Fi.

Một Beacon frames bất kì, ta dễ dàng thấy được SSID là **ns-3-ssid**.



## Tìm các gói tin thể hiện quá trình kết nối giữa các node và AP. Các thông điệp này có ý nghĩa gì?

Đây là ví dụ về quá trình kết nối giữa Station có MAC (00:00:00:00:00:01) và AP (00:00:00:00:00:06).



1. AP gửi Beacon frames để quảng bá về mạng Wi-Fi cũng như thông tin về Wi-Fi.
2. Station gửi một Association Request frame đến AP để yêu cầu kết nối. Chứa thông tin về station, địa chỉ MAC và SSID.
3. AP gửi một Acknowledgement frame để xác nhận đã nhận Association Request.
4. AP trả lời bằng một Association Response frame để trả lời Association Request của Station. Chứa thông tin về AP, địa chỉ MAC và SSID.
5. Station gửi một Acknowledgement frame để xác nhận đã nhận Association Response.

Sau khi hoàn thành các bước trên, station sẽ được kết nối với AP.

**CF-END** được sử dụng trong quá trình kết nối để đảm bảo rằng chỉ có một station có thể gửi gói tin Association Request frame tại một thời điểm. Nếu có nhiều station gửi gói tin Association Request frame cùng lúc, thì sẽ xảy ra xung đột. CF-END được sử dụng để xác định thời điểm kết thúc của giai đoạn xung đột và để cho phép các station khác gửi gói tin Association Request frame.

## Tìm hiểu quá trình khởi tạo kết nối UDP và chỉ ra các gói tin UDP đi từ client đến server và ngược lại. Giải thích sự tương quan giữa code và file .pcap.

### Quá trình khởi tạo kết nối UDP

Trước gửi các gói tin Station sẽ thiết lập **BA** session (Block ACK session). Sau khi thiết lập **BA** session, Station có thể gửi gói tin **BA** đến **AP** để nhóm nhiều frame thành một gói tin duy nhất. Một số lợi ích của việc sử dụng **BA** session như tăng băng thông, giảm độ trễ, cải thiện độ tin cậy.

Để thiết lập **BA** session ta cần hai gói tin Action với **Action Code** là **Add Block ACK Request (ADDBA Request)** và **Add Block ACK Response (ADDBA Response).**

**ADDBA Request** được gửi từ station đến AP để yêu cầu thiết lập BA session.

A screenshot of a computer

Description automatically generated

**ADDBA Response** được gửi bởi AP đến station để phản hồi gói tin ADDBA Request.

A screenshot of a computer

Description automatically generated

Các gói tin **Acknowledgement** ở hình trên được dung để phản hồi lại cho bên gửi rằng đã nhận được gói tin thành công. Sau 2 bước trên thì Client đã thiết lập thành công BA session đến APvà bắt đầu gửi gói tin ARP Boardcast để hỏi địa chỉ của server có IP 10.1.1.5 đến AP.

A screenshot of a computer

Description automatically generated

Khi AP nhận được gói tin ARP Boardcast thì sẽ forward đến toàn bộ Station đã kết nối.

A screenshot of a computer

Description automatically generated

Khi Server nhận được gói tin ARP Boardcast thì sẽ phản hồi địa chỉ MAC của mình cho Client thông qua AP, tuy nhiên trước đó Server và AP cũng sẽ phải thiết lập BA Seasion.

A screenshot of a computer

Description automatically generated

BA Sesion chỉ thiết lập một chiều cho nên khi truyền từ AP đến Client thì AP cũng phải thiết lập BA Sesion từ AP đến Client, các bước thiết lập cũng như mô tả ở trên. Sua khi toàn tất thiết lập gói tin ARP từ Server đã được gửi đến Client.

A screenshot of a computer

Description automatically generated

Sau khi có đủ thông tin Client sẽ bắt đầu gửi gói tin đến Hello đến Server thông qua AP, AP phản hồi lại gói tin Acknowledgement cho Client xác nhận đã nhận được gói tin. AP forward gói tin này đến Server tuy nhiên trước đó AP và Server chưa thiết lập BA Sesion nên phải thực hiện thiết lập kết nối.

A screenshot of a computer

Description automatically generated

Sau khi đã thiết lập BA Sesion AP gửi gói tin từ Client đến cho Server. Server phản hồi lại gói tin Acknowledgement cho AP xác nhận đã nhận được gói tin.

A screenshot of a computer

Description automatically generated

Khi Server trả lời gói tin Hello từ Client các bước cũng tương tự như Client gửi gói tin Hello đến Server. Đâu tiên Server gửi Broadcast hỏi địa chỉ của Client, sau khi có địa chỉ Server phản hồi gói tin UDP về cho Client. Tuy nhiên không cần thiết lập BA Sesion vì toàn bộ kết nối cần thiết đã được thiết lập khi Client gửi gói tin đến Server.



A screenshot of a computer

Description automatically generated

### Tương quan giữa code và file .pcap.



Trong code ta có nWifi = 5.



Và ta thấy ở đây index của udp Server là (nWifi – 1) = 4 và index của udp Client là 1.

A screen shot of a computer program

Description automatically generated+ Nên ta thấy IP của udp Server và udp Client sẽ phụ thuộc vào chỉ số index này.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Index | 0 | 1 | 2 | 3 | 4 |
| Đuôi của IP | .1 | .2 | .3 | .4 | .5 |

IP của Server là đuôi .5 và IP của Client là đuôi .2

A screenshot of a computer

Description automatically generated



## Khoảng thời gian giữa các lần truyền Beacon frames là bao nhiêu? Hãy chứng minh điều đó.

A screenshot of a computer screen

Description automatically generated

Trong hình ta có 4 lần truyền Beacon frames.

* Lần 2 cách lần 1: 0.1024 - 0.0000 = 0.1024s
* Lần 3 cách lần 2: 0.2048 - 0.1024 = 0.1024s
* Lần 4 cách lần 3: 0.3072 - 0.2048 = 0.1024s

Vậy suy ra thời gian giữa các lần truyền Beacon frames sẽ cố định ở mức 0.1024s.

## Địa chỉ MAC nguồn, đích, BSSID trong 802.11 frame có giá trị bao nhiêu (dưới dạng thập lục phân)? Chúng có ý nghĩa như thế nào và chiếm bao nhiêu bytes trong cấu trúc gói tin?

Địa chỉ nguồn (00:00:00\_00:00:05). Đây là địa chỉ MAC của station gửi gói tin. Địa chỉ MAC nguồn chiếm 6 bytes (48 bits) trong cấu trúc gói tin 802.11 frame.

A screenshot of a computer

Description automatically generated

Địa chỉ đích (00:00:00\_00:00:02). Đây là địa chỉ MAC của station nhận gói tin. Địa chỉ MAC đích cũng chiếm 6 bytes (48 bits) trong cấu trúc gói tin 802.11 frame.

A screen shot of a computer code

Description automatically generated

Địa chỉ MAC BSSID (00:00:00\_00:00:06). Đây là địa chỉ MAC của Access Point (AP) trong mạng Wi-Fi. BSSID được sử dụng để xác định nguồn, gốc AP của gói tin. BSSID cũng chiếm 6 bytes (48 bits) trong cấu trúc gói tin 802.11 frame.

A screenshot of a computer code

Description automatically generated

## Trong các Beacon frames quảng bá rằng có thể hỗ trợ nhiều data rates khác nhau, tìm các thông tin này? Cho biết các rates này có ý nghĩa gì?

Data rate là tốc độ truyền dữ liệu giữa AP và station. Data rate được đo bằng megabit trên giây (Mbps). Danh sách các data rates trong Supported Rates cho biết AP có thể hỗ trợ các tốc độ truyền dữ liệu nào. Station sẽ chọn data rate tối đa mà cả AP và station đều hỗ trợ.

Trong hình Beacon frames này có thể hỗ trợ 8 data rates khác nhau.

A white background with black text

Description automatically generated

* 6 Mbps
* 9 Mbps
* 12 Mbps
* 18 Mbps
* 24 Mbps
* 36 Mbps
* 48 Mbps
* 54 Mbps

Station sẽ chọn data rate tối đa mà cả AP và station đều hỗ trợ. Nếu station hỗ trợ tất cả các data rates trong danh sách, thì station sẽ chọn data rate 54 Mbps.

## Có tổng cộng bao nhiêu AP xung quanh, SSID của các AP này là gì? Hãy chứng minh điều đó.

Mở file pcap bằng WireShark vào mục Wireless -> Wireless Lan Stats. Ta thấy có tổng cộng 36 AP xung quanh.

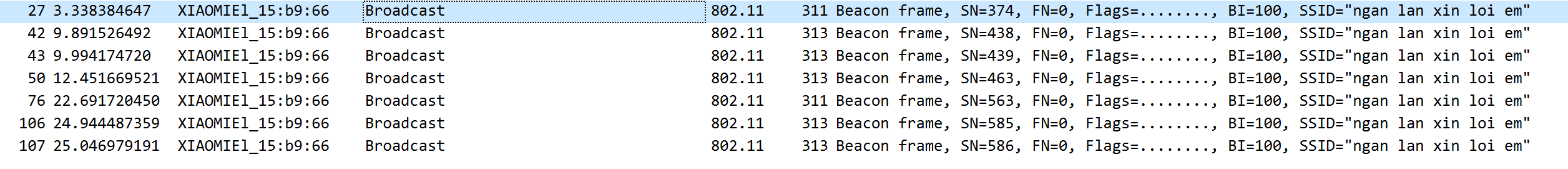
SSID của các AP này cũng chính là tên của các AP này.

A screenshot of a computer

Description automatically generated

## Thực hiện lại các câu hỏi 6, 7, 8. Các trường / nội dung này có gì đặt biệt, khác nhau giữa 2 kịch bản.

### Khoảng thời gian giữa các lần truyền Beacon frames là bao nhiêu? Hãy chứng minh điều đó.



Thời gian giữa các lần truyền là:

* Lần 2 cách lần 1: 0.582549208 - 0.582292748 = 0.00025646s + Lần 2 cách lần 1: 9.891526492 – 3.338384647 = 6.553141845s
* Lần 3 cách lần 2: 0.582791560 - 0.582549208 = 0.000242352s + Lần 3 cách lần 2: 9.994174720 - 9.891526492 = 0.102648228s
* Lần 5 cách lần 4: 21.832944998 – 21.832033980 = 0.002293471s + Lần 4 cách lần 3: 12.451669521 – 9.994174720 = 2.457494801s

Thời gian giữa các lần truyền không cố định.

Thời gian truyền giữa cá Becon frame trong kịch bản là cố địch khác với thực tế là không cố định.

### Địa chỉ MAC nguồn, đích, BSSID trong 802.11 frame có giá trị bao nhiêu (dưới dạng thập lục phân)? Chúng có ý nghĩa như thế nào và chiếm bao nhiêu bytes trong cấu trúc gói tin?

Địa chỉ nguồn (50:64:2b:15:b9:66). Đây là địa chỉ MAC của station gửi gói tin. Địa chỉ MAC nguồn chiếm 6 bytes (48 bits) trong cấu trúc gói tin 802.11 frame.

A screenshot of a computer

Description automatically generated

Địa chỉ đích (28:11:a8:85:3d:f6). Đây là địa chỉ MAC của station nhận gói tin. Địa chỉ MAC đích cũng chiếm 6 bytes (48 bits) trong cấu trúc gói tin 802.11 frame.

A screenshot of a computer

Description automatically generated

Địa chỉ MAC BSSID (50:64:2b:15:b9:66). Đây là địa chỉ MAC của Access Point (AP) trong mạng Wi-Fi. BSSID được sử dụng để xác định nguồn, gốc AP của gói tin. BSSID cũng chiếm 6 bytes (48 bits) trong cấu trúc gói tin 802.11 frame.

A screenshot of a computer code

Description automatically generated

Thực tế ngoài địa chỉ MAC còn có tên của thiết bị khác so với kịch bản.

### Trong các Beacon frames quảng bá rằng có thể hỗ trợ nhiều data rates khác nhau, tìm các thông tin này? Cho biết các rates này có ý nghĩa gì?

Data rate là tốc độ truyền dữ liệu giữa AP và station. Data rate được đo bằng megabit trên giây (Mbps). Danh sách các data rates trong Supported Rates cho biết AP có thể hỗ trợ các tốc độ truyền dữ liệu nào. Station sẽ chọn data rate tối đa mà cả AP và station đều hỗ trợ.

Trong hình Beacon frames này có thể hỗ trợ 8 data rates khác nhau.

A screenshot of a computer

Description automatically generated

* 6 Mbps
* 9 Mbps
* 12 Mbps
* 18 Mbps
* 24 Mbps
* 36 Mbps
* 48 Mbps
* 54 Mbps

Station sẽ chọn data rate tối đa mà cả AP và station đều hỗ trợ. Nếu station hỗ trợ tất cả các data rates trong danh sách, thì station sẽ chọn data rate 54 Mbps.

## Tìm các gói tin Probe Request và Probe Response trong các 802.11 frames. Mục đích của các gói tin này dùng để làm gì? Địa chỉ MAC nguồn, đích, BSSID của chúng như thế nào?

### Gói tin Probe Request

**Gói tin Probe Request** được gửi bởi các thiết bị Wi-Fi để tìm kiếm các AP. Gói tin này chứa các thông tin cơ bản về thiết bị, chẳng hạn như SSID, BSSID, và các thông số kỹ thuật hỗ trợ.

Có hai loại gói tin Probe Request:

* **Direct Probe Request:** Gói tin này chứa thông tin về một SSID cụ thể mà thiết bị đang tìm kiếm.
* **Null Probe Request:** Gói tin này không chứa thông tin về bất kỳ SSID nào.

A screenshot of a computer

Description automatically generated

Địa chỉ MAC nhận: 70:9c:d1:f1:88:c6

Địa chỉ MAC đích: 70:9c:d1:f1:88:c6

Địa chỉ MAC nguồn: bc:e6:7c:5a:c5:80

Tác dụng của các địa chỉ này đã được đề cập ở trên.

A screenshot of a computer

Description automatically generated

### Gói tin Prob Response

**Gói tin Probe Response** được gửi bởi các AP để đáp ứng các gói tin Probe Request. Gói tin này chứa các thông tin về AP, chẳng hạn như SSID, BSSID, cường độ tín hiệu, kênh, và các thông số bảo mật.

Có hai loại gói tin Probe Response:

* **Probe Response:** Gói tin này được gửi bởi các AP khi nhận được gói tin Probe Request.
* **Beacon:** Gói tin này được gửi bởi các AP định kỳ để quảng bá sự hiện diện của mình. Gói tin Beacon cũng chứa các thông tin tương tự như gói tin Probe Response.

A screenshot of a computer

Description automatically generated

Địa chỉ MAC nhận: 70:9c:d1:f1:88:c6

Địa chỉ MAC đích: 70:9c:d1:f1:88:c6

Địa chỉ MAC nguồn: bc:e6:7c:5a:c5:80

A screenshot of a computer

Description automatically generated

## Tìm cặp gói tin Authentication được gửi từ client đến AP và ngược lại, cho biết chúng dùng để làm gì? Các trường Authentication Algorithm, Authentication SEQ, Satatus code trong các gói tin Authentication ở trên thể hiện điều gì?

### Cặp gói tin Authentication.

Gói tin gửi từ Client đến AP.

A screenshot of a computer

Description automatically generated

Gói tin gửi từ AP đến Client.

A screenshot of a computer

Description automatically generated

### Các trường Authentication.

Trong các gói tin Authentication, các trường Authentication Algorithm, Authentication SEQ, và Status code thể hiện các thông tin sau:

* **Authentication Algorithm:** Đây là trường xác định thuật toán xác thực được sử dụng. Các thuật toán xác thực phổ biến bao gồm Open System Authentication (OSA), Shared Key Authentication (SKA), và WPA/WPA2 Authentication.
* **Authentication SEQ:** Đây là trường xác định thứ tự của các gói tin Authentication.
* **Status code:** Đây là trường xác định trạng thái của quá trình xác thực.

Dưới đây là giải thích chi tiết về từng trường:

**Authentication Algorithm**

Trường Authentication Algorithm xác định thuật toán xác thực được sử dụng. Các thuật toán xác thực phổ biến bao gồm:

* Open System Authentication (OSA): Đây là thuật toán xác thực đơn giản nhất, trong đó thiết bị truy cập (STA) chỉ cần gửi một gói tin Authentication Request đến điểm truy cập (AP). AP sẽ chấp nhận kết nối nếu STA có thể cung cấp thông tin xác thực chính xác.
* Shared Key Authentication (SKA): Đây là thuật toán xác thực mạnh hơn OSA, trong đó STA và AP chia sẻ một khóa bí mật. STA sử dụng khóa này để tạo một mã xác thực (MIC) cho gói tin Authentication Request. AP sẽ chấp nhận kết nối nếu MIC là chính xác.
* WPA/WPA2 Authentication: Đây là các thuật toán xác thực an toàn hơn SKA, sử dụng các thuật toán mã hóa và băm mạnh hơn.

**Authentication SEQ**

Trường Authentication SEQ xác định thứ tự của các gói tin Authentication. Các gói tin Authentication được gửi theo thứ tự tăng dần của giá trị Authentication SEQ.

**Status code**

Trường Status code xác định trạng thái của quá trình xác thực. Các mã trạng thái phổ biến bao gồm:

* 0: Thành công: Quá trình xác thực thành công.
* 1: Thất bại: Quá trình xác thực thất bại.
* 2: Yêu cầu xác thực lại: AP yêu cầu STA gửi lại gói tin Authentication Request.
* 3: Yêu cầu cung cấp thông tin xác thực bổ sung: AP yêu cầu STA cung cấp thêm thông tin xác thực.

## Tìm các gói tin Association được gửi từ client và ngược lại, trường thông tin nào cho biết chúng là một Association Request hay một Association Response? Tìm các thông tin Capabilities Information, SSID, rates supported trong Association Request và cho biết chúng có ý nghĩa như thế nào?

Association Request được sử dụng để yêu cầu kết nối với mạng Wi-Fi, trong khi Association Response được sử dụng để phản hồi yêu cầu kết nối. Các gói tin này giúp các thiết bị Wi-Fi và AP kết nối với nhau một cách an toàn và hiệu quả.

Để biết được nó là một Association Request hay Association Response ta có thể nhìn vào Type/Subtype của gói tin này.

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

Trong gói tin Association Request, các trường Capabilities Information, SSID, và rates supported thể hiện các thông tin sau:

* **Capabilities Information:** Đây là trường xác định các tính năng và khả năng của thiết bị truy cập (STA).
* **SSID:** Đây là tên của mạng Wi-Fi mà STA muốn kết nối.
* **rates supported:** Đây là danh sách các tốc độ dữ liệu mà STA hỗ trợ.

A screenshot of a computer

Description automatically generated

## Giữa Association Request và Association Response có xuất hiện thêm trường gì đặt biệt? Giá trị của nó là bao nhiêu?

Giữa Association Request và Association Response có xuất hiện thêm các trường đặc biệt PHY type, Short preamble, Channel, Frequency, Signal strength và TSF timestamp.

* **PHY type** là trường xác định loại PHY được sử dụng bởi AP.
* **Short preamble** là trường xác định AP có hỗ trợ preamble ngắn hay không. Preamble ngắn là một tính năng tiết kiệm năng lượng có thể được sử dụng để giảm độ trễ kết nối.
* **Channel** là trường xác định kênh Wi-Fi mà AP đang sử dụng.
* **Frequency** là trường xác định tần số của kênh Wi-Fi mà AP đang sử dụng.
* **Signal strength** là trường xác định cường độ tín hiệu của AP.
* **TSF timestamp** là trường xác định thời gian đã trôi qua kể từ khi AP được bật.

Các trường đặc biệt này giúp STA và AP xác định thông tin chi tiết về môi trường Wi-Fi và đảm bảo rằng kết nối Wi-Fi được thiết lập một cách an toàn và hiệu quả.

## Từ các nội dung đã tìm hiểu, trình bày quá trình WLAN 802.11 hoạt động thông qua các gói tin và sự khác nhau giữa kịch bản 1 và kịch bản 2.

|  |  |  |
| --- | --- | --- |
|  | **Kịch bản 1: (ns-3)** | **Kịch bản 2: (wireshark)** |
| **Giống Nhau** | - Phát sóng Beacon Frame: Access Point trong mạng Wi-Fi phát sóng các gói tin Beacon Frame định kỳ. Các Beacon Frame chứa thông tin về mạng, bao gồm SSID, khả năng bảo mật, tốc độ truyền dữ liệu, và thời gian chống trễ.  - Thiết bị Client Tìm Kiếm AP: Các thiết bị client trong phạm vi của mạng Wi-Fi gửi các gói Probe Request để tìm các mạng Wi-Fi có sẵn trong phạm vi của nó. Nó là cách để thiết bị tìm hiểu về mạng Wi-Fi xung quanh và có thể chọn mạng mà nó muốn kết nối.  - Client Gửi Association Request: Một thiết bị client quyết định kết nối vào mạng Wi-Fi cụ thể và gửi một gói tin "Association Request" đến AP của mạng đó. Gói tin này chứa thông tin về khả năng của client và yêu cầu kết nối.  - AP Gửi Association Response: AP nhận được gói tin "Association Request" và kiểm tra thông tin từ client. Nếu thông tin hợp lệ, AP sẽ gửi gói tin "Association Response" cho client để xác nhận việc kết nối.  - Client và AP trao đổi Dữ Liệu: Khi việc kết nối được thiết lập thành công, client và AP có thể gửi và nhận dữ liệu qua mạng Wi-Fi. Dữ liệu được chia thành các gói tin và truyền qua kênh không dây.  - Các Gói Tin Management và Control: Ngoài việc truyền dữ liệu, WLAN 802.11 còn sử dụng các gói tin quản lý (management) và kiểm soát (control) để duy trì kết nối và quản lý mạng. Điều này bao gồm gói tin như Request to Send (RTS), Clear to Send (CTS), ACK | |
| **Khác nhau** | - Tập trung vào mô phỏng và hiểu cách hoạt động của mạng Wi-Fi trong một môi trường kiểm soát.  - Tùy chỉnh các thông số, thời gian thực hiện thí nghiệm. -> hiệu suất và cho ra kết quả tốt và nhanh hơn.  - Đánh giá và kiểm tra hiệu suất mạng trong điều kiện kiểm soát và tái tạo các tình huống đặc biệt. | **-** Theo dõi và bắt các gói tin thực tế trong mạng WLAN 802.11 thực sự. Ta không kiểm soát được mạng, chỉ có thể quan sát và phân tích dữ liệu.  - Hiểu sâu về cách mà mạng thực tế hoạt động, bao gồm các yếu tố như nhiễu, sự cạnh tranh trên kênh tần số và các vấn đề hiệu suất .  - Ta có thể đánh giá 1 cách khách quan mô hình mạng, từ đó có các sự chuẩn bị, điều chỉnh phù hợp để thích nghi với môi trường |

# TÀI LIỆU THAM KHẢO

[ns-3 Tutorial](https://www.nsnam.org/docs/tutorial/html/)

[WikiPedia IEEE 802.11](https://en.wikipedia.org/wiki/IEEE_802.11)

UIT’s NT131 Slide