BÁO CÁO THỰC HÀNH

Môn học: Hệ thống nhúng mạng không dây

Buổi báo cáo: Lab 1

Tên chủ đề: Tìm hiểu WLAN 802.11

GVHD: Nguyễn Văn Bảo

Ngày thực hiện: 27/3/2024

THÔNG TIN CHUNG:

(Liệt kê tất cả các thành viên trong nhóm)
Lớp: NT131.O21.2

STT	Họ và tên	MSSV	Email
1	Nguyễn Đình Luân	21521105	21521105@gm.uit.edu.vn

1. **ĐÁNH GIÁ KHÁC:**

Nội dung	Kết quả
Tổng thời gian thực hiện bài thực hành trung bình	
Link Video thực hiện *(nếu có)*	
Ý kiến *(nếu có)* + Khó khăn + Đề xuất …	
Điểm tự đánh giá	8

BÁO CÁO CHI TIẾT

1. **Câu hỏi 1**

Giải thích code:

Thiết lập số lượng wifi:

```
uint32_t nWifi = 5;
CommandLine cmd;
cmd.AddValue ("nWifi", "Number of wifi STA devices", nWifi);
cmd.Parse (argc,argv);
```

Kiểm tra số lượng wifi liệu có hợp lệ:

```
if (nWifi > 250)
  {
    std::cout << "Too many wifi nodes, no more than 250 each." << std::endl;
    return 1;
  }
```

Tạo các node wifi cần thiết lập ap:

```
NodeContainer wifiStaNodes;
wifiStaNodes.Create(nWifi);
NodeContainer wifiApNode = wifiStaNodes.Get(0);
```

Tạo và thiết lập kênh truyền, kênh lỗi cho wifi

```
YansWifiChannelHelper channel = YansWifiChannelHelper::Default ();
YansWifiPhyHelper phy;
phy.SetErrorRateModel ("ns3::NistErrorRateModel");
phy.SetChannel (channel.Create ());
```

Thiết lập thông số wifi

```
WifiHelper wifi;
wifi.SetRemoteStationManager ("ns3::AarfWifiManager");
```

Thiết lập địa chỉ MAC cho thiết bị wifi. Loại MAC được thiết lập là “StaWifiMac” và SSID là “ns-3-ssid”

```
WifiMacHelper mac;
Ssid ssid = Ssid ("ns-3-ssid");
mac.SetType ("ns3::StaWifiMac",
             "Ssid", SsidValue (ssid),
             "ActiveProbing", BooleanValue (false));
```

Thiết lập và kết nối thiết bị wifi với mạng

```
NetDeviceContainer staDevices;
staDevices = wifi.Install (phy, mac, wifiStaNodes);

mac.SetType ("ns3::ApWifiMac",
             "Ssid", SsidValue (ssid));

NetDeviceContainer apDevices;
apDevices = wifi.Install (phy, mac, wifiApNode);
```

Thiết lập Vị trí và cách thức di chuyển của các thiết bị wifi

```
mobility.SetPositionAllocator ("ns3::GridPositionAllocator",
                               "MinX", DoubleValue (0.0),
                               "MinY", DoubleValue (0.0),
                               "DeltaX", DoubleValue (5.0),
                               "DeltaY", DoubleValue (10.0),
                               "GridWidth", UintegerValue (3),
                               "LayoutType", StringValue ("RowFirst"));

mobility.SetMobilityModel ("ns3::RandomWalk2dMobilityModel",
                           "Bounds", RectangleValue (Rectangle (-50, 50, -50, 50)));
mobility.Install (wifiStaNodes);

mobility.SetMobilityModel ("ns3::ConstantPositionMobilityModel");
mobility.Install (wifiApNode);
```

Cấu hình giao thức mạng internet trên các thiết bị bằng InternetStackHelper. Sau đó cấp phát địa chỉ IP thông qua Ipv4Address và Assign. Cuối cùng, bảng định tuyến được cập nhật thông qua Ipv4GlobalRoutingHelper::PopulaeRoutingTables

```
InternetStackHelper stack;
stack.Install (wifiStaNodes);
Ipv4AddressHelper address;

address.SetBase ("10.1.1.0", "255.255.255.0");
Ipv4InterfaceContainer wifiInterfaces;
wifiInterfaces = address.Assign (staDevices);
address.Assign (apDevices);

UdpEchoServerHelper echoServer (9);

ApplicationContainer serverApps = echoServer.Install (wifiStaNodes.Get (nWifi - 1));
serverApps.Start (Seconds (1.0));
serverApps.Stop (Seconds (10.0));

UdpEchoClientHelper echoClient (wifiInterfaces.GetAddress (nWifi - 1), 9);
echoClient.SetAttribute ("MaxPackets", UintegerValue (1));
echoClient.SetAttribute ("Interval", TimeValue (Seconds (1.0)));
echoClient.SetAttribute ("PacketSize", UintegerValue (1024));

ApplicationContainer clientApps =
echoClient.Install (wifiStaNodes.Get (1));
clientApps.Start (Seconds (2.0));
clientApps.Stop (Seconds (10.0));

Ipv4GlobalRoutingHelper::PopulateRoutingTables ();
```

Về kịch bản:

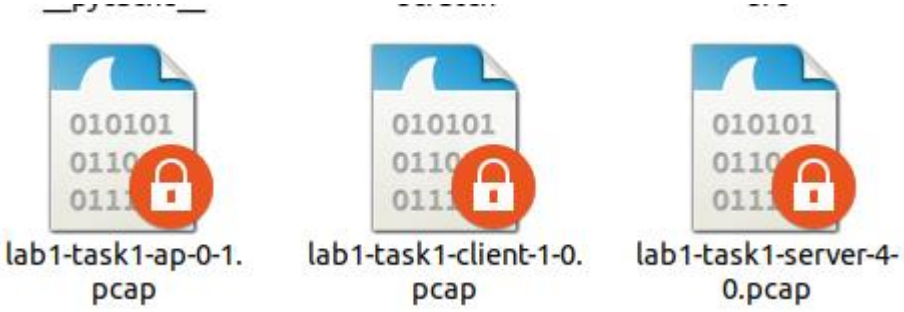
Có 5 thiết bị wifi và một trong số đó là access point.

Có 1 máy là udp client ở node 2 và udp server ở node 5. 2 máy này sẽ gửi dữ liệu cho nhau

2. Câu hỏi 2

Thêm đoạn code sau vào file .cc để có thể log ra 3 file:

```
phy.EnablePcap("lab1-task1-ap", apDevices.Get(0));
phy.EnablePcap("lab1-task1-server", staDevices.Get(nWifi - 1));
phy.EnablePcap("lab1-task1-client", staDevices.Get(1));
```



3. Câu hỏi 3:

Trong mạng không dây Wi-Fi chuẩn 802.11, các Beacon frames là các gói tin mà các Access Point (AP) gửi ra để thông báo sự tồn tại của mạng Wi-Fi đó.

Các Beacon frames chứa các thông tin quan trọng như:

- SSID (Service Set Identifier): Đây là tên của mạng Wi-Fi, cho phép các thiết bị khách xác định và kết nối với mạng mong muốn.
- BSSID (Basic Service Set Identifier): Đây là địa chỉ duy nhất của điểm truy cập (AP) trên mạng Wi-Fi.
- Thông số kỹ thuật: Beacon frames cung cấp các thông số kỹ thuật như tốc độ truyền, chuẩn Wi-Fi (như 802.11ac, 802.11n), kênh sử dụng, và các thông số khác để các thiết bị khách có thể tương thích và thiết lập kết nối đúng cách.
- Thời gian: Beacon frames cung cấp thông tin về thời gian hệ thống của điểm truy cập, giúp đồng bộ hóa thời gian giữa các thiết bị trong mạng.
- Các thông báo quảng cáo: Beacon frames có thể chứa các thông báo quảng cáo như thông tin về dịch vụ, sản phẩm, hoặc sự kiện quan trọng liên quan đến mạng hoặc tổ chức.

Beacon frame trong mạng Wi-Fi 802.11 có ý nghĩa quan trọng như sau:

- Thông báo sự tồn tại của mạng: Beacon frame giúp các thiết bị di động nhận biết và xác định sự tồn tại của một mạng Wi-Fi trong phạm vi phủ sóng của nó.

- Cung cấp thông tin cơ bản về mạng: Beacon frame chứa các thông tin như tên mạng (SSID), chế độ hoạt động, tốc độ truyền dữ liệu, mã hóa bảo mật, và các thông số khác liên quan đến cấu hình mạng.

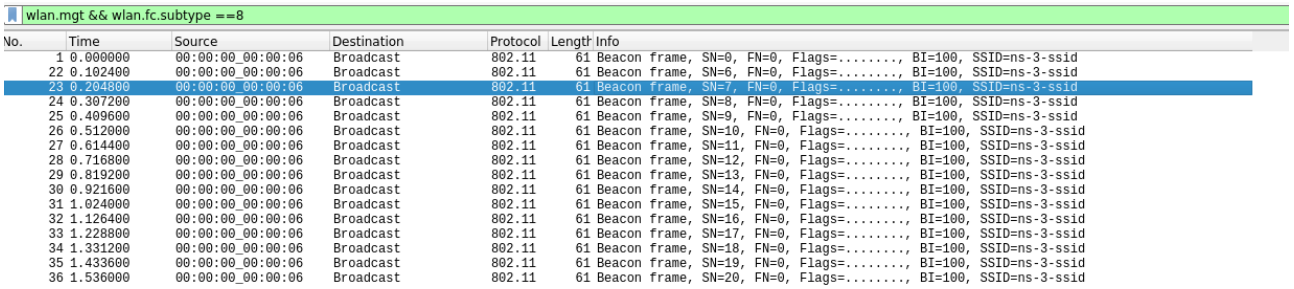
- Hỗ trợ di động và roaming: Các Beacon frame cung cấp thông tin về các Access Point khác trong cùng một mạng, giúp thiết bị di động có thể chuyển đổi giữa các AP một cách mượt mà và duy trì kết nối khi di chuyển qua các vùng phủ sóng khác nhau.

- Đồng bộ hóa thời gian: Beacon frame có thể chứa thông tin về thời gian, giúp các thiết bị trong mạng đồng bộ hóa thời gian của họ.

- Tạo điểm đồng bộ cho mạng: Beacon frame được sử dụng để đồng bộ hóa thời gian truyền thông giữa các thiết bị trong mạng, giúp tăng hiệu suất truyền dữ liệu và đảm bảo tính ổn định của mạng.

Tóm lại, Beacon frame không chỉ thông báo sự tồn tại của mạng Wi-Fi mà còn chứa các thông tin quan trọng giúp thiết bị di động kết nối và duy trì kết nối mạng một cách hiệu quả.

SSID của ap là ns-3-ssid



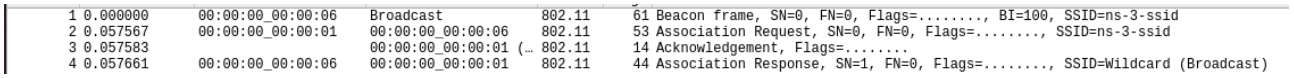
wlan.mgt && wlan.fc.subtype ==8

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	00:00:00_00:00:06	Broadcast	802.11	61	Beacon frame, SN=0, FN=0, Flags=........, BI=100, SSID=ns-3-ssid
22	0.102400	00:00:00_00:00:06	Broadcast	802.11	61	Beacon frame, SN=6, FN=0, Flags=........, BI=100, SSID=ns-3-ssid
23	0.204800	00:00:00_00:00:06	Broadcast	802.11	61	Beacon frame, SN=7, FN=0, Flags=........, BI=100, SSID=ns-3-ssid
24	0.307200	00:00:00_00:00:06	Broadcast	802.11	61	Beacon frame, SN=8, FN=0, Flags=........, BI=100, SSID=ns-3-ssid
25	0.409600	00:00:00_00:00:06	Broadcast	802.11	61	Beacon frame, SN=9, FN=0, Flags=........, BI=100, SSID=ns-3-ssid
26	0.512000	00:00:00_00:00:06	Broadcast	802.11	61	Beacon frame, SN=10, FN=0, Flags=........, BI=100, SSID=ns-3-ssid
27	0.614400	00:00:00_00:00:06	Broadcast	802.11	61	Beacon frame, SN=11, FN=0, Flags=........, BI=100, SSID=ns-3-ssid
28	0.716800	00:00:00_00:00:06	Broadcast	802.11	61	Beacon frame, SN=12, FN=0, Flags=........, BI=100, SSID=ns-3-ssid
29	0.819200	00:00:00_00:00:06	Broadcast	802.11	61	Beacon frame, SN=13, FN=0, Flags=........, BI=100, SSID=ns-3-ssid
30	0.921600	00:00:00_00:00:06	Broadcast	802.11	61	Beacon frame, SN=14, FN=0, Flags=........, BI=100, SSID=ns-3-ssid
31	1.024000	00:00:00_00:00:06	Broadcast	802.11	61	Beacon frame, SN=15, FN=0, Flags=........, BI=100, SSID=ns-3-ssid
32	1.126400	00:00:00_00:00:06	Broadcast	802.11	61	Beacon frame, SN=16, FN=0, Flags=........, BI=100, SSID=ns-3-ssid
33	1.228800	00:00:00_00:00:06	Broadcast	802.11	61	Beacon frame, SN=17, FN=0, Flags=........, BI=100, SSID=ns-3-ssid
34	1.331200	00:00:00_00:00:06	Broadcast	802.11	61	Beacon frame, SN=18, FN=0, Flags=........, BI=100, SSID=ns-3-ssid
35	1.433600	00:00:00_00:00:06	Broadcast	802.11	61	Beacon frame, SN=19, FN=0, Flags=........, BI=100, SSID=ns-3-ssid
36	1.536000	00:00:00_00:00:06	Broadcast	802.11	61	Beacon frame, SN=20, FN=0, Flags=........, BI=100, SSID=ns-3-ssid

4. Câu hỏi 4:

Quá trình kết nối diễn ra như sau:

- AP gửi broadcast gói tin beacon frame cho các node
- Node sẽ quét mạng và nhận các gói tin beacon frame từ các AP. Khi đã chọn được AP (AP mạnh nhất), nó sẽ gửi gói tin Association Request chứa thông tin để yêu cầu kết nối tới AP đó
- AP sẽ kiểm tra thông tin của gói Association Request, nếu các thông tin hợp lệ, yêu cầu kết nối được chấp nhận thì AP sẽ gửi gói Association Response cho node để thông báo kết nối được chấp nhận

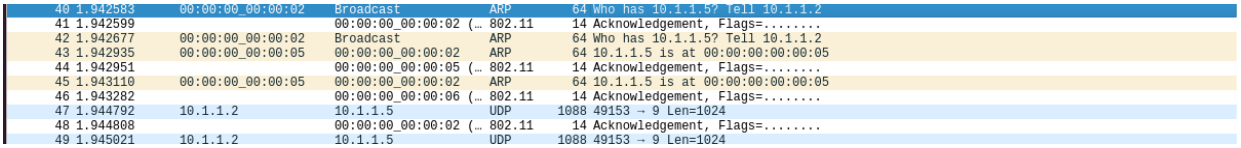


1	0.000000	00:00:00_00:00:06	Broadcast	802.11	61 Beacon frame, SN=0, FN=0, Flags=........, BI=100, SSID=ns-3-ssid
2	0.057567	00:00:00_00:00:01	00:00:00_00:00:06	802.11	53 Association Request, SN=0, FN=0, Flags=........, SSID=ns-3-ssid
3	0.057583		00:00:00_00:00:01 (…	802.11	14 Acknowledgement, Flags=........
4	0.057661	00:00:00_00:00:06	00:00:00_00:00:01	802.11	44 Association Response, SN=1, FN=0, Flags=........, SSID=Wildcard (Broadcast)

5. Câu hỏi 5

Udp không tạo ra kết nối mà gửi trực tiếp gói tin đến ip đích, nhưng trước đó cần phải gửi gói tin arp để lấy được địa chỉ mac ở đích

ARP (Address Resolution Protocol): được sử dụng trong mạng máy tính để tìm địa chỉ MAC (Media Access Control) tương ứng với địa chỉ IP của một thiết bị trong cùng mạng con. Gói tin ARP được sử dụng để xác định địa chỉ MAC của một thiết bị trong mạng trước khi gửi các gói tin đến thiết bị đó.

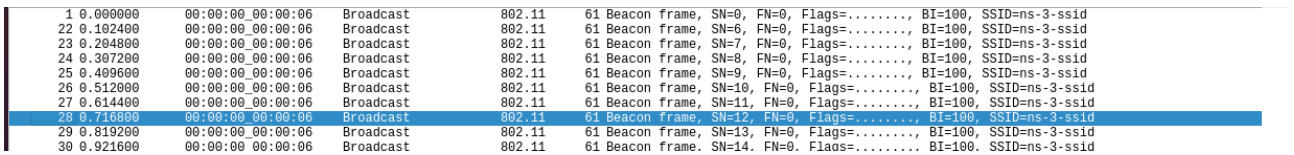


40	1.942583	00:00:00_00:00:02	Broadcast	ARP	64 Who has 10.1.1.5? Tell 10.1.1.2
41	1.942599		00:00:00_00:00:02 (…	802.11	14 Acknowledgement, Flags=........
42	1.942677	00:00:00_00:00:02	Broadcast	ARP	64 Who has 10.1.1.5? Tell 10.1.1.2
43	1.942935	00:00:00_00:00:05	00:00:00_00:00:02	ARP	64 10.1.1.5 is at 00:00:00:00:00:05
44	1.942951		00:00:00_00:00:05 (…	802.11	14 Acknowledgement, Flags=........
45	1.943110	00:00:00_00:00:05	00:00:00_00:00:02	ARP	64 10.1.1.5 is at 00:00:00:00:00:05
46	1.943282		00:00:00_00:00:06 (…	802.11	14 Acknowledgement, Flags=........
47	1.944792	10.1.1.2	10.1.1.5	UDP	1088 49153 → 9 Len=1024
48	1.944808		00:00:00_00:00:02 (…	802.11	14 Acknowledgement, Flags=........
49	1.945021	10.1.1.2	10.1.1.5	UDP	1088 49153 → 9 Len=1024

Như trên hình, ở gói tin 43, gói arp được gửi broadcast để hỏi địa chỉ mac và kết quả được trả về ip 10.1.1.2 ở gói tin 43, sau đó, gói tin udp đầu tiên được gửi là gói tin số 47

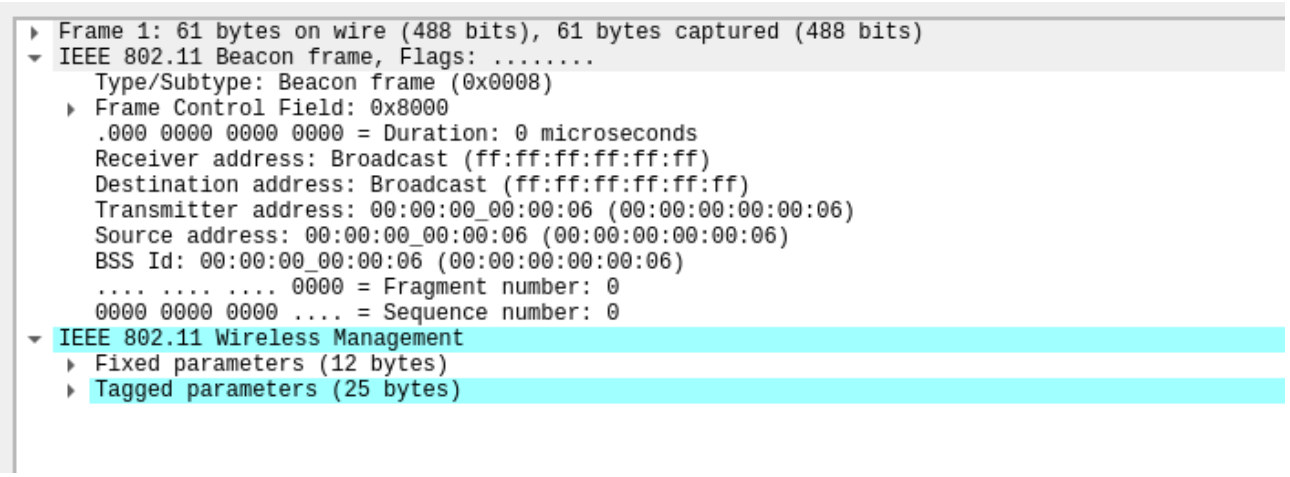
6. Câu hỏi 6

Khoảng thời gian giữa các lần truyền Beacon frames là 0.1024 giây
Ta lấy thời gian của gói beacon frame sau trừ gói beacon frame trước:



1	0.000000	00:00:00_00:00:06	Broadcast	802.11	61 Beacon frame, SN=0, FN=0, Flags=........, BI=100, SSID=ns-3-ssid
22	0.102400	00:00:00_00:00:06	Broadcast	802.11	61 Beacon frame, SN=6, FN=0, Flags=........, BI=100, SSID=ns-3-ssid
23	0.204800	00:00:00_00:00:06	Broadcast	802.11	61 Beacon frame, SN=7, FN=0, Flags=........, BI=100, SSID=ns-3-ssid
24	0.307200	00:00:00_00:00:06	Broadcast	802.11	61 Beacon frame, SN=8, FN=0, Flags=........, BI=100, SSID=ns-3-ssid
25	0.409600	00:00:00_00:00:06	Broadcast	802.11	61 Beacon frame, SN=9, FN=0, Flags=........, BI=100, SSID=ns-3-ssid
26	0.512000	00:00:00_00:00:06	Broadcast	802.11	61 Beacon frame, SN=10, FN=0, Flags=........, BI=100, SSID=ns-3-ssid
27	0.614400	00:00:00_00:00:06	Broadcast	802.11	61 Beacon frame, SN=11, FN=0, Flags=........, BI=100, SSID=ns-3-ssid
28	0.716800	00:00:00_00:00:06	Broadcast	802.11	61 Beacon frame, SN=12, FN=0, Flags=........, BI=100, SSID=ns-3-ssid
29	0.819200	00:00:00_00:00:06	Broadcast	802.11	61 Beacon frame, SN=13, FN=0, Flags=........, BI=100, SSID=ns-3-ssid
30	0.921600	00:00:00_00:00:06	Broadcast	802.11	61 Beacon frame, SN=14, FN=0, Flags=........, BI=100, SSID=ns-3-ssid

7. Câu hỏi 7



Địa chỉ MAC nguồn: 00:00:00:00:00:06

Địa chỉ MAC đích: ff:ff:ff:ff:ff:ff

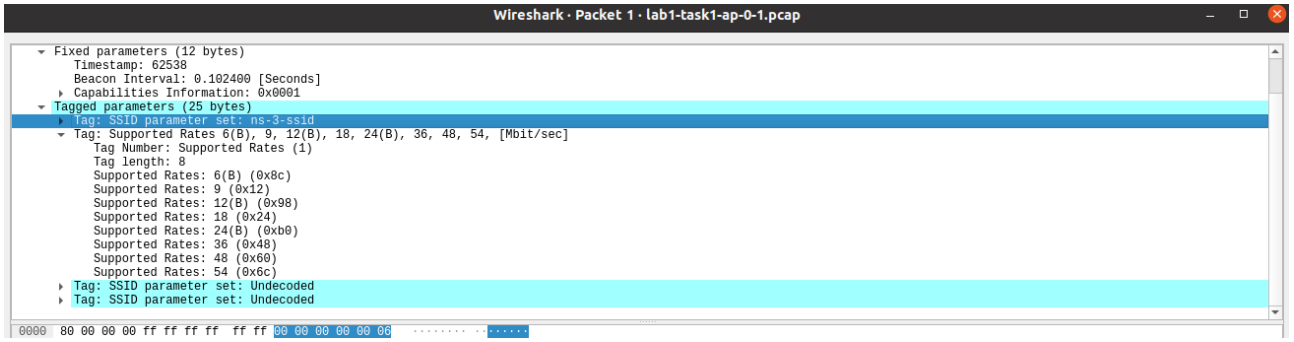
BSSID: 00:00:00:00:00:06

Trong các gói tin 802.11 frame, các địa chỉ MAC nguồn (source), đích (destination) và BSSID được biểu diễn dưới dạng thập lục phân (hexadecimal). Dưới đây là ý nghĩa và số lượng bytes của mỗi địa chỉ trong cấu trúc gói tin 802.11:

- Địa chỉ MAC nguồn (source MAC address):
  - Ý nghĩa: Đây là địa chỉ MAC của thiết bị gửi gói tin.
  - Kích thước: Địa chỉ MAC nguồn chiếm 6 bytes trong cấu trúc gói tin 802.11.
  - Biểu diễn thập lục phân: Dạng xx:xx:xx:xx:xx:xx.
- Địa chỉ MAC đích (destination MAC address):
  - Ý nghĩa: Đây là địa chỉ MAC của thiết bị nhận gói tin.
  - Kích thước: Địa chỉ MAC đích cũng chiếm 6 bytes trong cấu trúc gói tin 802.11.
  - Biểu diễn thập lục phân: Dạng xx:xx:xx:xx:xx:xx.
- BSSID (Basic Service Set Identifier):
  - Ý nghĩa: BSSID là địa chỉ MAC của Access Point (AP) hoặc Router mà thiết bị kết nối đến trong mạng không dây.
  - Kích thước: BSSID cũng có kích thước 6 bytes trong gói tin 802.11.
  - Biểu diễn thập lục phân: Dạng xx:xx:xx:xx:xx:xx.

Với mỗi loại địa chỉ, các giá trị thập lục phân được biểu diễn bằng cặp số hex, mỗi cặp tương ứng với một byte. Số lượng bytes của mỗi địa chỉ là 6 bytes, do đó, tổng số bytes để biểu diễn tất cả các địa chỉ trong một gói tin 802.11 là 6 + 6 + 6 = 18 bytes.

8. Câu hỏi 8



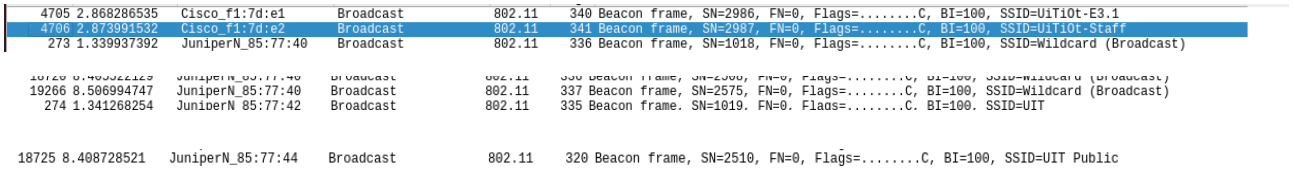
Trường "Support Rate" trong Beacon frame của mạng Wi-Fi (802.11) chứa danh sách các tốc độ truyền dữ liệu mà Access Point (AP) hoặc điểm truy cập có khả năng hỗ trợ. Cụ thể, trường này chứa các giá trị của các tốc độ dữ liệu mà thiết bị có thể sử dụng để truyền và nhận dữ liệu từ mạng Wi-Fi.

Mỗi giá trị trong trường "Support Rate" thường được biểu diễn bằng 1 byte và đại diện cho một tốc độ truyền dữ liệu cụ thể, được biểu thị dưới dạng số thập phân hoặc số hexa. Các tốc độ truyền dữ liệu thường được ghi bằng Mbps (Megabits per second).

Trường "Support Rate" giúp thiết bị trong phạm vi phủ sóng của mạng Wi-Fi biết được các tốc độ dữ liệu mà Access Point hỗ trợ. Điều này cho phép các thiết bị di động lựa chọn tốc độ tối ưu khi kết nối vào mạng, cũng như đảm bảo tính tương thích giữa các thiết bị trong mạng Wi-Fi.

Ví dụ, một trường "Support Rate" có thể chứa các giá trị như 1, 2, 5.5, 11, 18, 24, 36, 48, 54, thể hiện các tốc độ truyền dữ liệu được hỗ trợ bởi Access Point tương ứng.

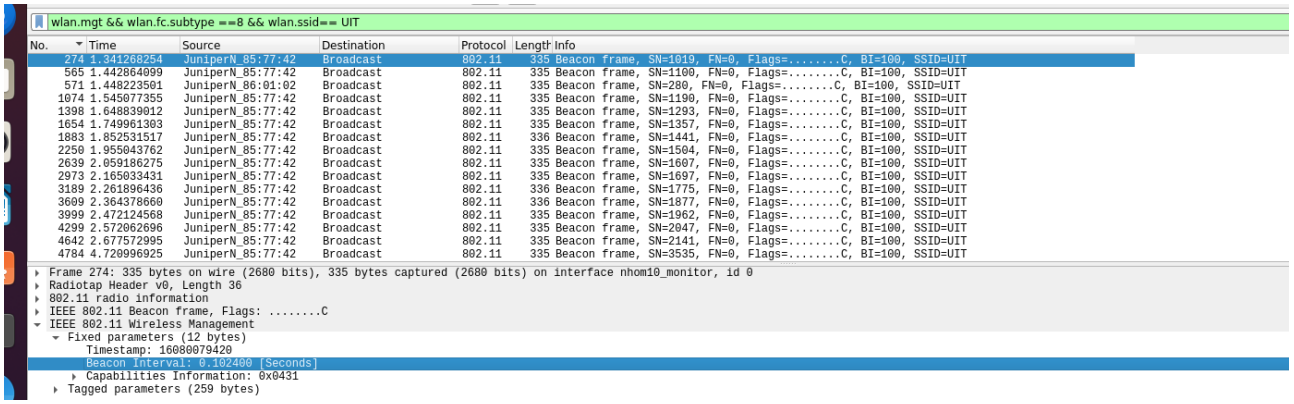
9. Câu hỏi 9



Có 5 AP xung quanh và ssid của chúng là: UIT, UIT public, wildcard, UiTiOt-E3.1, UiTiOt-Staff.

10. Câu hỏi 10

Khoảng thời gian giữa các lần truyền Beacon frames là 0.1024 giây, điều này được thể hiện trong trường beacon interval. Trường này là một phần quan trọng của gói tin Beacon và có mục đích xác định khoảng thời gian giữa các lần phát sóng Beacon frame của một Access Point



Địa chỉ MAC nguồn là: dc:38:e1:85:77:42

Địa chỉ MAC đích là: ff:ff:ff:ff:ff:ff

```
IEEE 802.11 Beacon frame, Flags: ........C
    Type/Subtype: Beacon frame (0x0008)
  ▸ Frame Control Field: 0x8000
    .000 0000 0000 0000 = Duration: 0 microseconds
    Receiver address: Broadcast (ff:ff:ff:ff:ff:ff)
    Destination address: Broadcast (ff:ff:ff:ff:ff:ff)
    Transmitter address: JuniperN_85:77:42 (dc:38:e1:85:77:42)
    Source address: JuniperN_85:77:42 (dc:38:e1:85:77:42)
    BSS Id: JuniperN_85:77:42 (dc:38:e1:85:77:42)
    .... .... .... 0000 = Fragment number: 0
    0110 1110 1111 .... = Sequence number: 1775
    Frame check sequence: 0x786d8bf4 [unverified]
    [FCS Status: Unverified]
```

Các Data rate mà UIT hỗ trợ:

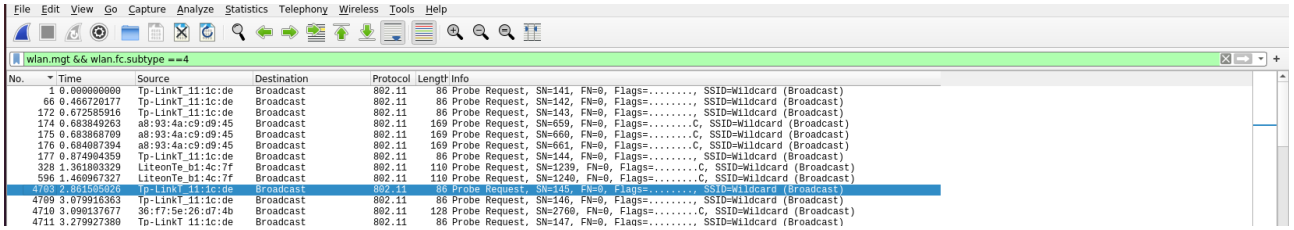
```
    Tag length: 3
    SSID: UIT
▾ Tag: Supported Rates 1(B), 2(B), 5.5(B), 6, 9, 11(B), 12, 18, [Mbit/sec]
    Tag Number: Supported Rates (1)
    Tag length: 8
    Supported Rates: 1(B) (0x82)
    Supported Rates: 2(B) (0x84)
    Supported Rates: 5.5(B) (0x8b)
    Supported Rates: 6 (0x0c)
    Supported Rates: 9 (0x12)
    Supported Rates: 11(B) (0x96)
    Supported Rates: 12 (0x18)
    Supported Rates: 18 (0x24)
▾ Tag: DS Parameter set: Current Channel: 11
    Tag Number: DS Parameter set (3)
```

Điểm khác nhau giữa kịch bản:

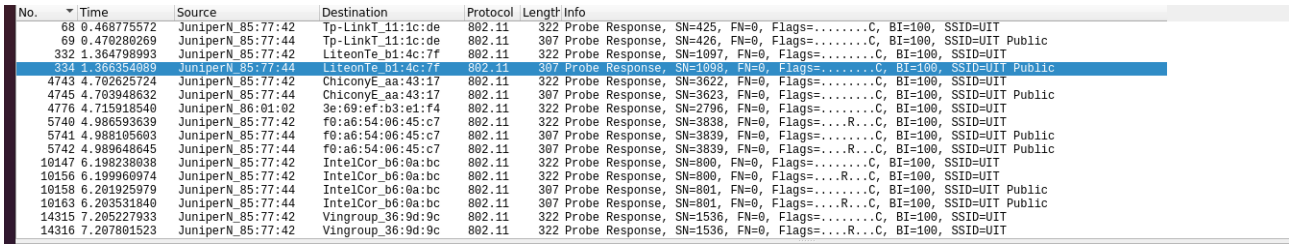
- Số AP tìm được ở hai kịch bản là khác nhau.
- Khoảng thời gian giữa các lần truyền Beacon frames của hai kịch bản có sự khác biệt:
  - Với kịch bản bắt gói tin bằng cách giả lập trên ns-3, khoảng thời gian luôn chính xác 0.1024 giây.
  - Với kịch bản thực tế bắt gói tin, khoảng thời gian không đồng đều.

11. Câu hỏi 11:

Các gói tin probe request:



Các gói tin probe respond:



- Gói tin Probe Request có thể chứa thông tin về một SSID nào đó, gọi là Direct Probe Request. Gói tin này được dùng khi client muốn tìm một SSID cụ thể. Khi AP nhận được gói tin này, và AP cũng được cấu hình SSID tương ứng, AP sẽ trả lời bằng gói tin Probe Response.
- Gói tin Probe Request cũng có thể không chứa bất kỳ thông tin nào về SSID, gọi là Null Probe Request. Khi client gửi gói tin này, tất cả AP sẽ trả lời bằng các gói tin Probe Response, chứa thông tin về tất cả SSID mà các AP này đang có.
- Địa chỉ MAC nguồn của gói Probe Request là của các client, Probe Respone là từ các AP.
- MAC đích của Probe Request có thể là broadcast hoặc địa chỉ của AP. Probe Response có MAC đích là của các client đã gửi Probe Resquest.
- BSSID sẽ là broadcast hoặc của AP

12. Câu hỏi 12:

Các trường trong Auth Frame:

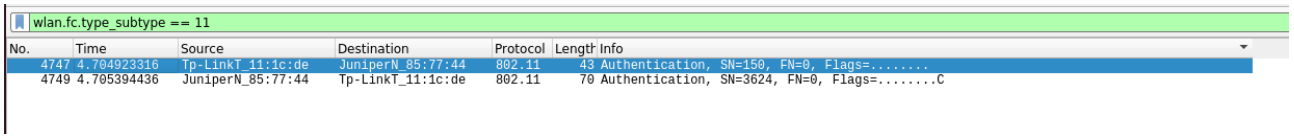
Authentication Algorithm là 0 đối với (Open System) – 1 cho Shared Key.

Authentication SEQ: thể hiện hiện trạng tiến độ - hay nó các khác nó là số thứ tự của các frame.

Status code: 0 thể hiện cho quá trình xác thực thành công và 1 là thất bại

Ngoài ra còn 1 trường challenge text sử dụng trong các tiến trình xác thực có sử dụng Shared Key.

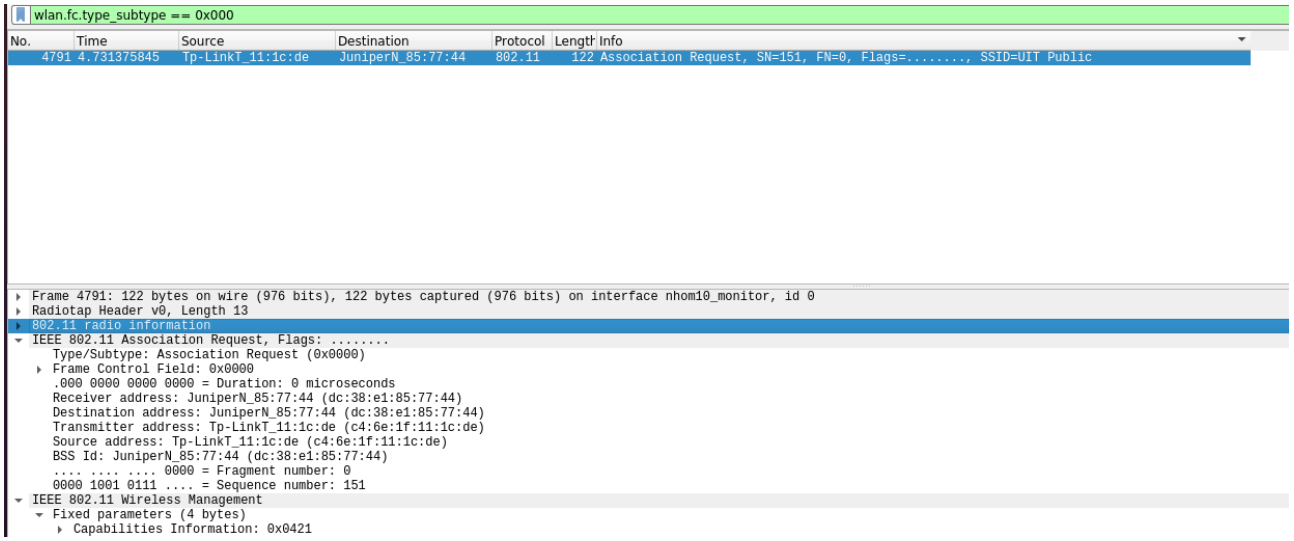
Tìm cặp gói tin Authentication từ client đến ap và ngược lại(Em không biết tại sao SEQ lại không trùng):



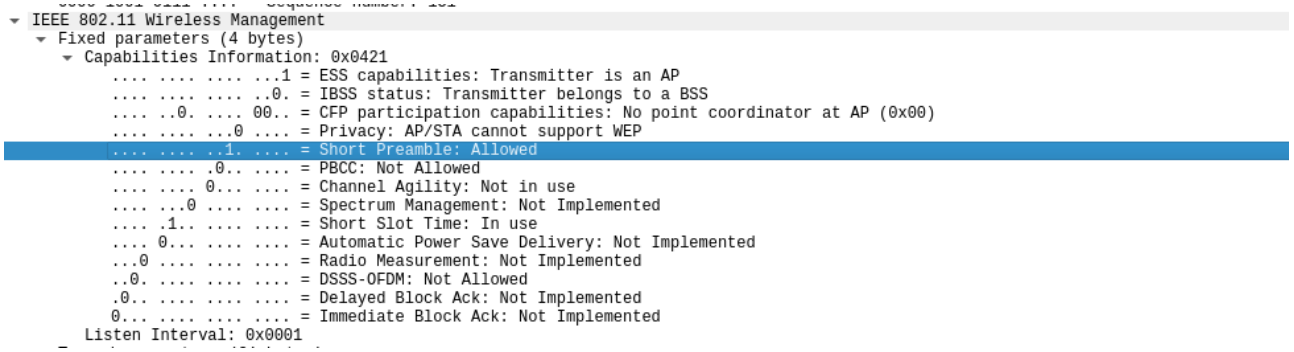
13. Câu hỏi 13

Trường type cho chúng ta biết nó loại frame nào. Đối với Assoocitation Resquest Frame có giá trịtype_subtype là 0x0000 và Association Response Frame là 0x0001.

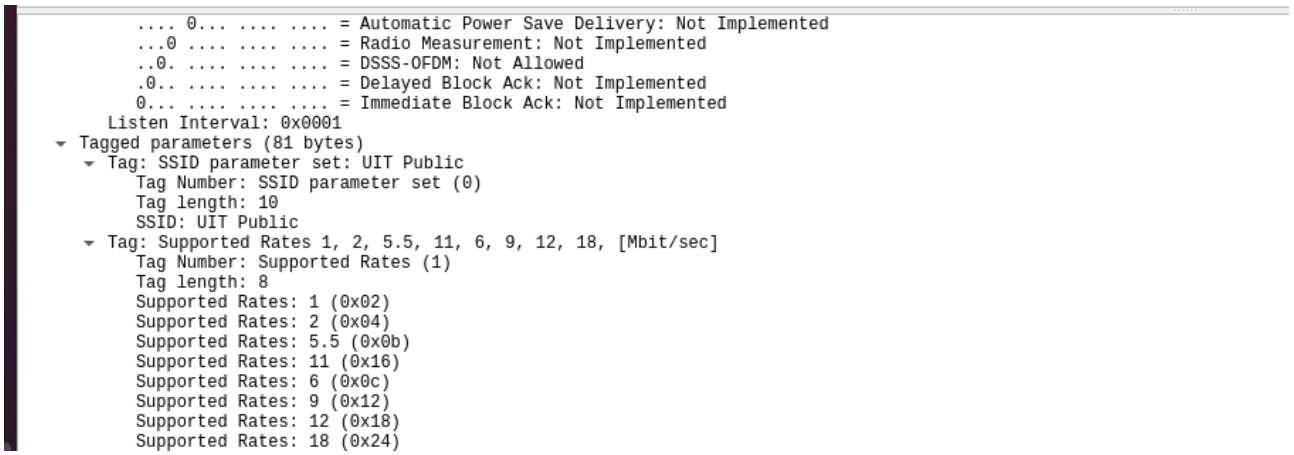
Gói tin assoiciation request từ client đến AP



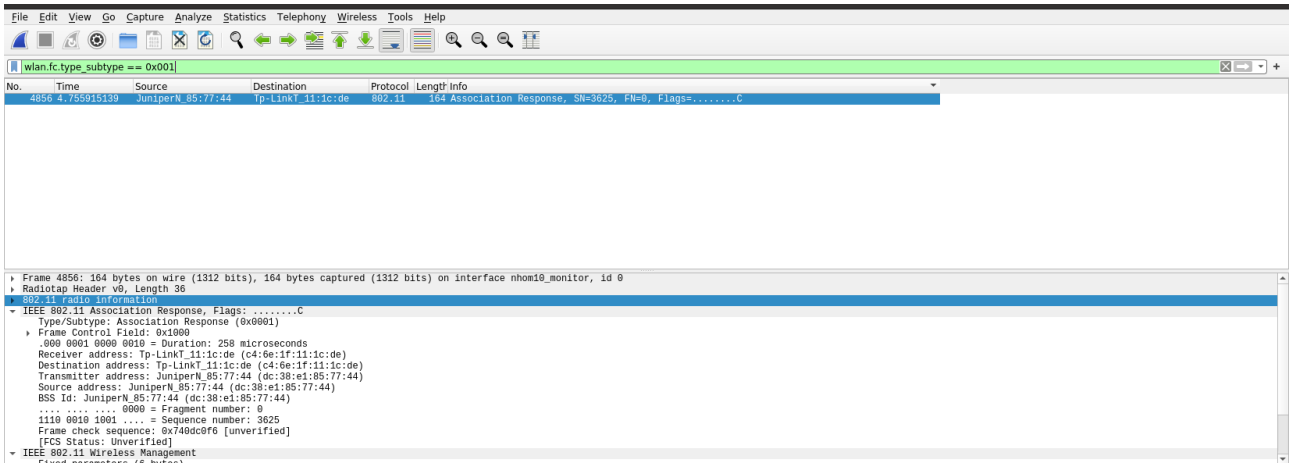
Câpbilities information:



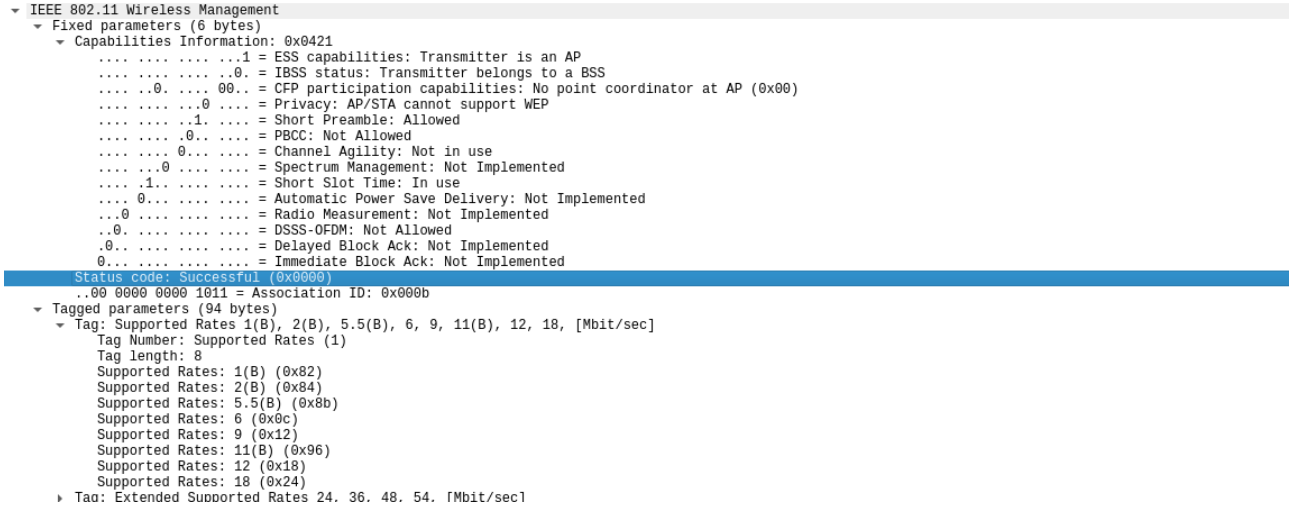
SSID và support rate:



Gói tin association response từ AP đến client



Capabilities Information và support rate:



Capabilities Information chứa các thông tin về khả năng của thiết bị, bao gồm các cờ (flags) dành cho các chức năng như hỗ trợ bảo mật WEP, hỗ trợ HT (High Throughput - dành cho chuẩn 802.11n), và các cờ khác.

SSID chứa tên của mạng wifi mà client muốn kết nối.

Supported Rates là danh sách các tốc độ truyền dữ liệu của mạng wifi mà thiết bị muốn tham gia.

14. Câu 14

Trong Association Req Frame có 1 trường là Listen Interval có giá trị là 0x0001. Trường này thể hiện khoảng thời gian nghỉ giữa các lần thức dậy của client để nghe các tín hiệu đã được buffer từ AP nhằm tiết kiệm năng lượng.

```
IEEE 802.11 Wireless Management
  Fixed parameters (4 bytes)
    Capabilities Information: 0x0421
        .... .... .... ...1 = ESS capabilities: Transmitter is an AP
        .... .... .... ..0. = IBSS status: Transmitter belongs to a BSS
        .... ..0. .... 00.. = CFP participation capabilities: No point coordinator at AP (0x00)
        .... .... ...0 .... = Privacy: AP/STA cannot support WEP
        .... .... ..1. .... = Short Preamble: Allowed
        .... .... .0.. .... = PBCC: Not Allowed
        .... .... 0... .... = Channel Agility: Not in use
        .... ...0 .... .... = Spectrum Management: Not Implemented
        .... .1.. .... .... = Short Slot Time: In use
        .... 0... .... .... = Automatic Power Save Delivery: Not Implemented
        ...0 .... .... .... = Radio Measurement: Not Implemented
        ..0. .... .... .... = DSSS-OFDM: Not Allowed
        .0.. .... .... .... = Delayed Block Ack: Not Implemented
        0... .... .... .... = Immediate Block Ack: Not Implemented
      Listen Interval: 0x0001
```

Association res frames có thêm trường status code, AID. Status code =0 nghĩa là kết nối thành công. Còn AID là mã định danh cho client khi kết nối thành công trong gói này có giá trị là 0x000b

```
IEEE 802.11 Wireless Management
  Fixed parameters (6 bytes)
    Capabilities Information: 0x0421
        .... .... .... ...1 = ESS capabilities: Transmitter is an AP
        .... .... .... ..0. = IBSS status: Transmitter belongs to a BSS
        .... ..0. .... 00.. = CFP participation capabilities: No point coordinator at AP (0x00)
        .... .... ...0 .... = Privacy: AP/STA cannot support WEP
        .... .... ..1. .... = Short Preamble: Allowed
        .... .... .0.. .... = PBCC: Not Allowed
        .... .... 0... .... = Channel Agility: Not in use
        .... ...0 .... .... = Spectrum Management: Not Implemented
        .... .1.. .... .... = Short Slot Time: In use
        .... 0... .... .... = Automatic Power Save Delivery: Not Implemented
        ...0 .... .... .... = Radio Measurement: Not Implemented
        ..0. .... .... .... = DSSS-OFDM: Not Allowed
        .0.. .... .... .... = Delayed Block Ack: Not Implemented
        0... .... .... .... = Immediate Block Ack: Not Implemented
    Status code: Successful (0x0000)
    ..00 0000 0000 1011 = Association ID: 0x000b
```

15. Câu hỏi 15:

Các giai đoạn hoạn động của Wlan 802.11:

Trước khi vào giai đoạn khởi tạo, các gói tin beacon sẽ được broadcast và các trạm sẽ dựa vào nó để biết xung quanh đang có các BSS nào.

1. Giai đoạn khởi tạo:

- Thiết bị muốn kết nối với mạng WLAN sẽ gửi tín hiệu dò tìm (probe request) để tìm kiếm các mạng Wi-Fi khả dụng.
- Các điểm truy cập (access point - AP) trong phạm vi sẽ gửi tín hiệu phản hồi dò tìm (probe response) chứa thông tin về mạng Wi-Fi của họ, bao gồm tên mạng (SSID), loại bảo mật, kênh truyền, v.v.

2. Giai đoạn xác thực:

- Thiết bị chọn mạng Wi-Fi muốn kết nối và gửi yêu cầu xác thực (authentication request) đến AP.
- AP sẽ kiểm tra tính hợp lệ của thông tin đăng nhập (tên người dùng và mật khẩu) được cung cấp bởi thiết bị.

- Nếu thông tin đăng nhập hợp lệ, AP sẽ gửi thông báo xác thực thành công (authentication response) cho thiết bị.

3. Giai đoạn liên kết:

- Thiết bị gửi yêu cầu liên kết (association request) đến AP.
- AP sẽ cấp cho thiết bị một địa chỉ MAC ảo (BSSID) và thông tin cấu hình mạng.
- Sau khi nhận được thông tin liên kết thành công (association response), thiết bị có thể bắt đầu truyền dữ liệu với các thiết bị khác trên mạng WLAN.

4. Giai đoạn truyền dữ liệu:

- Thiết bị sử dụng phương thức truy cập kênh truyền thông (medium access control - MAC) để chia sẻ kênh truyền một cách hiệu quả.
- Các phương thức MAC phổ biến bao gồm CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance) và OFDMA (Orthogonal Frequency Division Multiple Access).
- Thiết bị sẽ mã hóa dữ liệu trước khi truyền đi để đảm bảo bảo mật.

5. Giai đoạn kết thúc:

- Khi thiết bị muốn ngắt kết nối khỏi mạng WLAN, nó sẽ gửi yêu cầu hủy liên kết (disassociation request) đến AP.
- AP sẽ xác nhận việc hủy liên kết và xóa thông tin của thiết bị khỏi mạng.

Sự khác nhau giữa kịch bản giả lập và thực tế: trong kịch bản giả lập thì chỉ có các thiết bị mà chúng ta lập trình ra nên các khoản thời gian mà gói tin đến và các loại gói tin có trong file pcap luôn chính xác và đoán trước được nhưng với thực tế thì các gói tin này có thể bị nhiễu,... khiến cho thời gian đến có sai số.

YÊU CẦU CHUNG

1) Đánh giá

- Chuẩn bị tốt các yêu cầu đặt ra trong bài thực hành.
- Sinh viên hiểu và tự thực hiện được bài thực hành, trả lời đầy đủ các yêu cầu đặt ra.
- Nộp báo cáo kết quả chi tiết những đã thực hiện, quan sát thấy và kèm ảnh chụp màn hình kết quả *(nếu có)*; giải thích cho quan sát *(nếu có)*.
- Sinh viên báo cáo kết quả thực hiện và nộp bài.

2) Báo cáo

- File .PDF hoặc .docx. Tập trung vào nội dung, giải thích.
- Nội dung trình bày bằng Font chữ Times New Romans/ hoặc font chữ của mẫu báo cáo này (UTM Avo)– cỡ chữ 13. Canh đều (Justify) cho văn bản. Canh giữa (Center) cho ảnh chụp.
- Đặt tên theo định dạng: LabX_MSSV1. (trong đó X là Thứ tự buổi Thực hành).
  Ví dụ: Lab01_21520001
- Nộp file báo cáo trên theo thời gian đã thống nhất tại courses.uit.edu.vn.

Bài sao chép, trễ, … sẽ được xử lý tùy mức độ vi phạm.

HẾT