计算机学院 计算机网络 课程实验报告

实验题目： 802.11 WiFi		学号：202200130048
日期：5.21	班级： 6	姓名： 陈静雯
Email：1205037094@qq.com		

实验方法介绍：

通过 wireshark 研究 802.11 无线网络协议

实验过程描述：

1. 开始
2. 信标帧
3. 数据传输
4. Disassociation/Authentication/Association

结论分析：

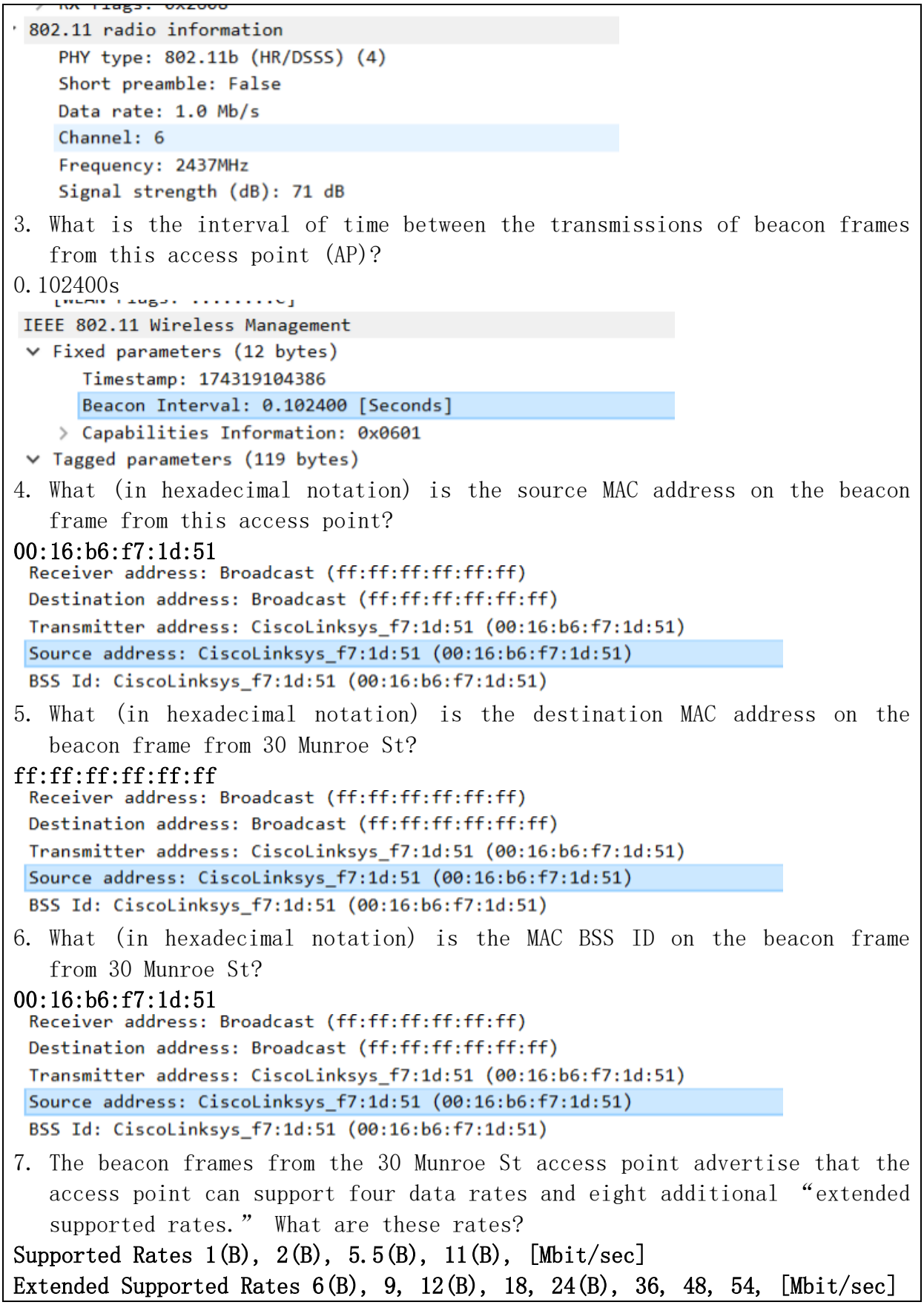
1. What are the SSIDs of the two access points that are issuing most of the beacon frames in this trace?

SSID=30 Munroe St

```
BI=100, SSID="30 Munroe St"
BI=100, SSID="30 Munroe St"
BI=100, SSID="30 Munroe St"
BI=100, SSID="30 Munroe St"
BI=62, SSID=6c69ee0104e2273a32[Malf
BI=100, SSID="30 Munroe St"
BI=100, SSID="30 Munroe St"
BI=100, SSID="linksys12"
BI=100, SSID="30 Munroe St"
BI=100, SSID="linksys12"
BI=100, SSID="30 Munroe St"
BI=100, SSID="30 Munroe St"
BI=100, SSID="30 Munroe St"
BI=100, SSID="30 Munroe St"
BI=100, SSID="linksys12"
BI=100, SSID="30 Munroe St"
BI=100, SSID=2cdc6e6b7379733132
```

2. What 802.11 channel is being used by both of these access points

channel=6



3. What is the interval of time between the transmissions of beacon frames from this access point (AP)?

0.102400s

4. What (in hexadecimal notation) is the source MAC address on the beacon frame from this access point?

00:16:b6:f7:1d:51

5. What (in hexadecimal notation) is the destination MAC address on the beacon frame from 30 Munroe St?

ff:ff:ff:ff:ff:ff

6. What (in hexadecimal notation) is the MAC BSS ID on the beacon frame from 30 Munroe St?

00:16:b6:f7:1d:51

7. The beacon frames from the 30 Munroe St access point advertise that the access point can support four data rates and eight additional "extended supported rates." What are these rates?

Supported Rates 1(B), 2(B), 5.5(B), 11(B), [Mbit/sec]
Extended Supported Rates 6(B), 9, 12(B), 18, 24(B), 36, 48, 54, [Mbit/sec]

```
Tagged parameters (119 bytes)
  Tag: SSID parameter set: "30 Munroe St"
  Tag: Supported Rates 1(B), 2(B), 5.5(B), 11(B), [Mbit/sec]
  Tag: DS Parameter set: Current Channel: 6
  Tag: Traffic Indication Map (TIM): DTIM 0 of 1 bitmap
  Tag: Country Information: Country Code US, Environment Indoor
  Tag: EDCA Parameter Set
  Tag: ERP Information
  Tag: Extended Supported Rates 6(B), 9, 12(B), 18, 24(B), 36, 48, 54, [Mbit/sec]
  Tag: Vendor Specific: Airgo Networks, Inc.
```

8. What are three MAC address fields in the 802.11 frame?

Source address、destination address、BSS Id

Which MAC address in this frame corresponds to the wireless host (give the hexadecimal representation of the MAC address for the host)?

SA：00:13:02:d1:b6:4f

To the access point?

BSS Id：00:16:b6:f7:1d:51

To the first-hop router?

Dst add：00:16:b6:f4:eb:a8

What is the IP address of the wireless host sending this TCP segment?

Source add：192.168.1.109

What is the destination IP address for the TCP syn segment?

Dst add：128.119.245.12

```
    .000 0000 0010 1100 = Duration: 44 microseconds
    Receiver address: CiscoLinksys_f7:1d:51 (00:16:b6:f7:1d:51)
    Transmitter address: Intel_d1:b6:4f (00:13:02:d1:b6:4f)
    Destination address: CiscoLinksys_f4:eb:a8 (00:16:b6:f4:eb:a8)
    Source address: Intel_d1:b6:4f (00:13:02:d1:b6:4f)
    BSS Id: CiscoLinksys_f7:1d:51 (00:16:b6:f7:1d:51)
    STA address: Intel_d1:b6:4f (00:13:02:d1:b6:4f)
    .... .... .... 0000 = Fragment number: 0
  [Header checksum status: Unverified]
  Source Address: 192.168.1.109
  Destination Address: 128.119.245.12
Transmission Control Protocol, Src Port: 2538, Dst Port: 80
```

9. Does the destination IP address of this TCP SYN correspond to the host, access point, first-hop router, or the destination web server?

TCP SYN 段的目的 IP 地址对应于目的地 Web 服务器。当一个客户端（如无线主机）初始化与 Web 服务器的 TCP 连接时，它会发送一个 SYN（同步）段，其中的目的 IP 地址是 Web 服务器的 IP 地址。这标志着客户端希望与该特定服务器建立通信。因此，该目的 IP 地址既不是客户端自己（无线主机），也不是中间的网络设备如接入点（AP）或第一跳路由器的 IP 地址。

10. Find the 802.11 frame containing the SYNACK segment for this TCP session received at t=24.8277 What are three MAC address fields in the 802.11 frame?

Source address、destination address、BSS Id

Which MAC address in this frame corresponds to the host?

SA：00:16:b6:f4:eb:a8

To the access point?

BSS：00:16:b6:f7:1d:51

To the first-hop router?

DST：91:2a:b0:49:b6:4f

Does the sender MAC address in the frame correspond to the IP address of the device that sent the TCP segment encapsulated within this datagram?

YES

```
Duration/ID: 11560 (reserved)
Receiver address: 91:2a:b0:49:b6:4f (91:2a:b0:49:b6:4f)
Transmitter address: CiscoLinksys_f7:1d:51 (00:16:b6:f7:1d:51)
Destination address: 91:2a:b0:49:b6:4f (91:2a:b0:49:b6:4f)
Source address: CiscoLinksys_f4:eb:a8 (00:16:b6:f4:eb:a8)
BSS Id: CiscoLinksys_f7:1d:51 (00:16:b6:f7:1d:51)
STA address: 91:2a:b0:49:b6:4f (91:2a:b0:49:b6:4f)
.... .... .... 0000 = Fragment number: 0
1100 0011 0100 .... = Sequence number: 3124
```

11. What two actions are taken (i.e., frames are sent) by the host in the trace just after t=49, to end the association with the 30 Munroe St AP that was initially in place when trace collection began?

802.11 层 - 解除关联请求：主机向 AP 发送一个解除关联请求帧。这个帧中包含了源 MAC 地址（主机的 MAC 地址）、目的 MAC 地址（AP 的 MAC 地址）以及表示请求解除关联的控制字段。此步骤正式告知 AP，主机希望断开与该 AP 的无线连接。

解除关联响应：在接收到解除关联请求后，30 Munroe St AP 会回复一个解除关联响应帧给主机。这个响应帧确认了 AP 已经接受了主机的解除关联请求，并且双方的关联状态正式结束。响应帧中同样包含了双方的 MAC 地址以及确认解除关联的控制信息。

IP 层动作 - DHCPRELEASE:虽然直接的 IP 层动作与解除无线关联（802.11 层的动作）不直接相关，但在实际场景中，主机可能随后会执行 DHCP RELEASE 过程来释放其从 DHCP 服务器获得的 IP 地址和其他网络配置信息。这是因为在断开与某个网络的连接之前，礼貌地释放 IP 地址是一个推荐的做法，以避免地址资源的浪费。DHCPRELEASE 报文是一个 IP 层的动作，它通过 UDP 协议发送到 DHCP 服务器，请求释放之前分配给该主机的 IP 地址租约。

```
1749 49.649705    Intel_d1:b6:4f    CiscoLinksys_f5:ba:… 802.11    58 Authentication, SN=1606, FN=0, Flags=....R...C
1750 49.651078    Intel_d1:b6:4f    CiscoLinksys_f5:ba:… 802.11   107 Association Request, SN=1607, FN=0, Flags=........C, SSID="linksys_SES_24
1751 49.653218    Intel_d1:b6:4f    CiscoLinksys_f5:ba:… 802.11   107 Association Request, SN=1607, FN=0, Flags=....R...C, SSID="linksys_SES_24
1732 49.542481    CiscoLinksys_f7:1d:… Broadcast          802.11   183 Beacon frame, SN=3588, FN=0, Flags=........C, E
1733 49.583615    192.168.1.109     192.168.1.1           DHCP     390 DHCP Release  - Transaction ID 0xea5a526
1734 49.583771                      Intel_d1:b6:4f (00:… 802.11    38 Acknowledgement, Flags=........C
1735 49.609617    Intel_d1:b6:4f    CiscoLinksys_f7:1d:… 802.11    54 Deauthentication, SN=1605, FN=0, Flags=........
```

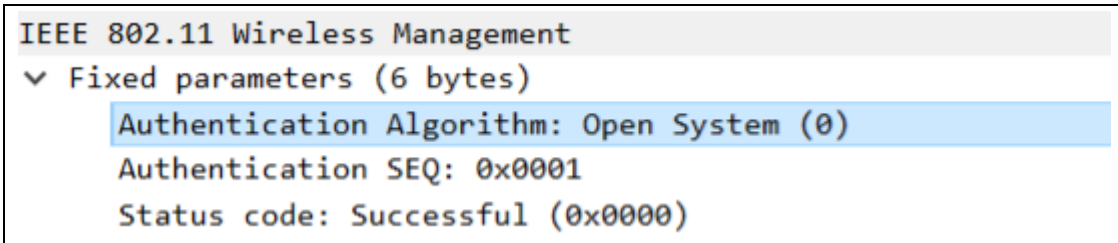
12. What form of authentication is the host requesting?

Open system

```
IEEE 802.11 Wireless Management
▾ Fixed parameters (6 bytes)
    Authentication Algorithm: Open System (0)
    Authentication SEQ: 0x0001
    Status code: Successful (0x0000)
```

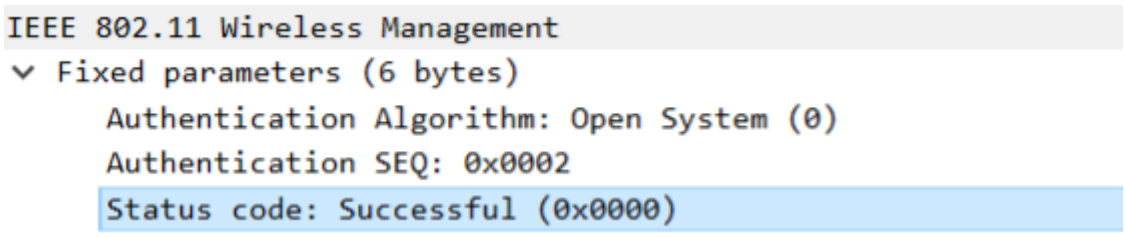
13. What is the Authentication SEQ value (authentication sequence number) of this authentication frame from host to AP?

SEQ：0x0001



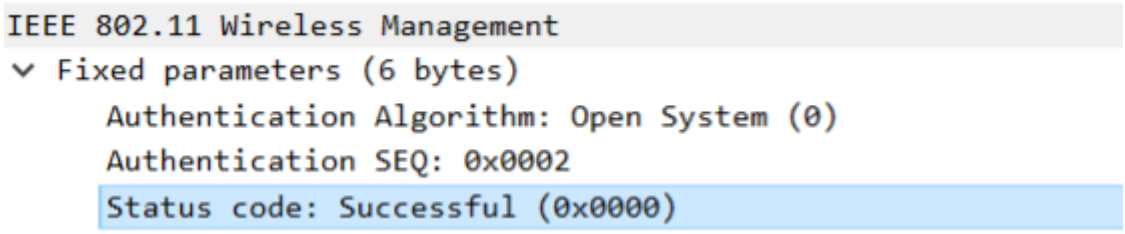
14. The AP response to the authentication request is received at t = 63.1690. Has the AP accepted the form of authentication requested by the host?

YES



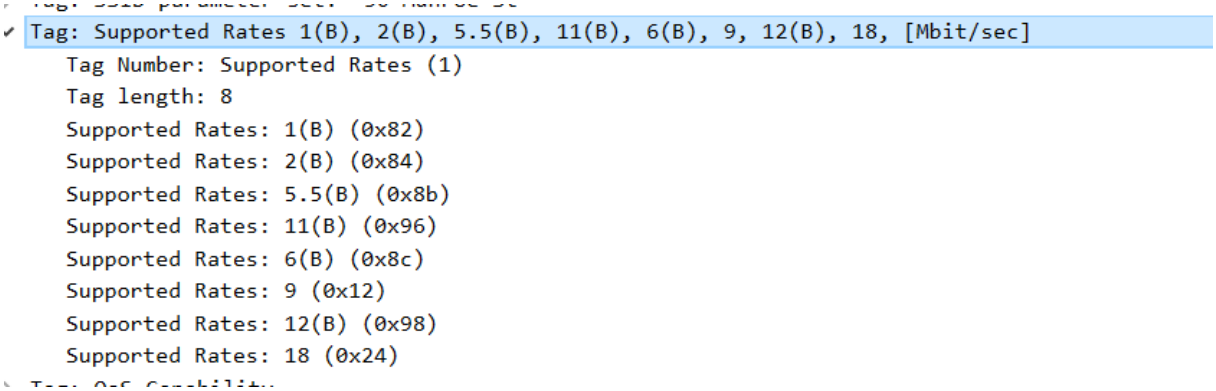
15. What is the Authentication SEQ value of this authentication frame from AP to Host?

0x0002



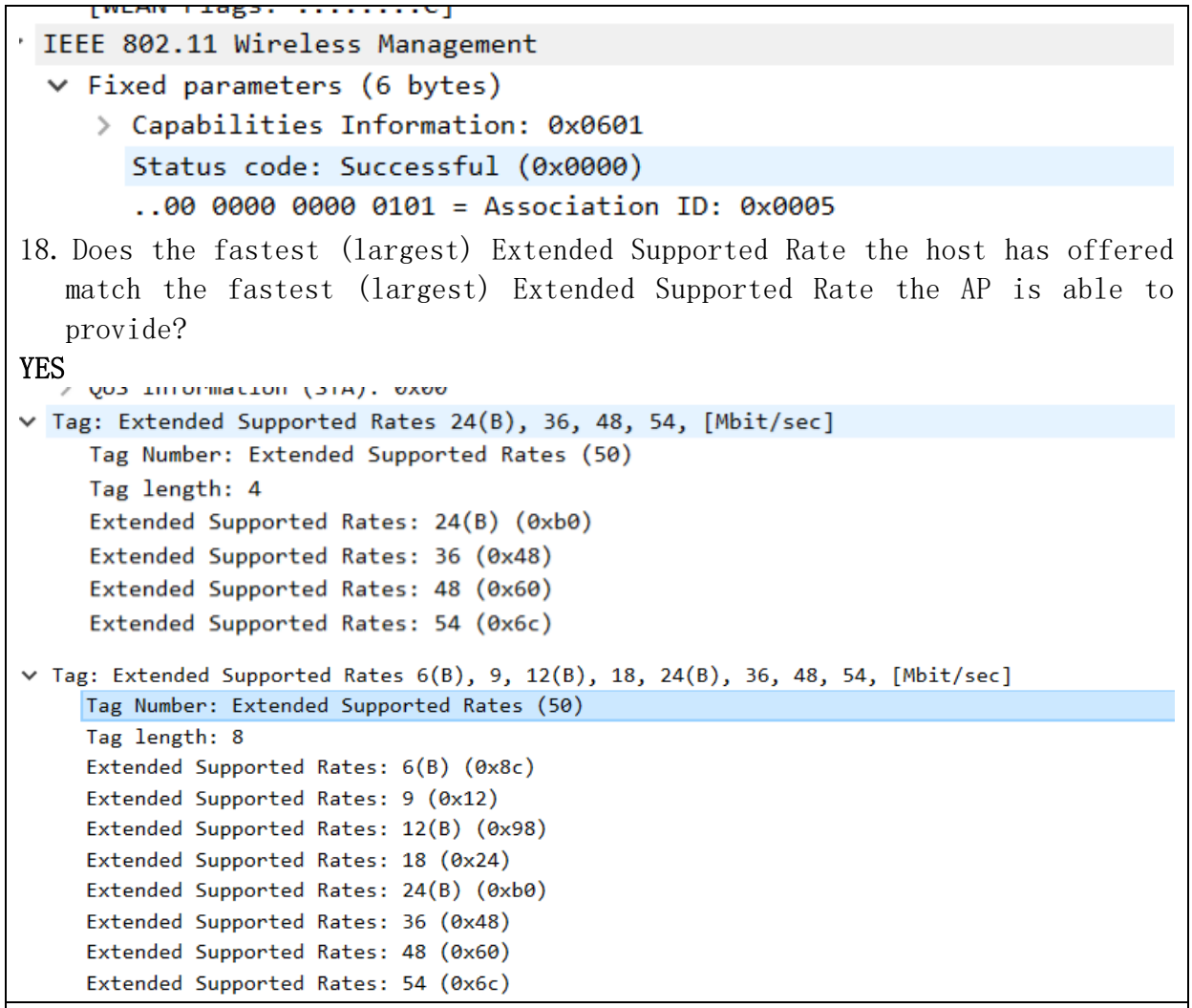
16. What rates are indicated in the frame as SUPPORTED RATES.

Supported Rates 1(B), 2(B), 5.5(B), 11(B), 6(B), 9, 12(B), 18, [Mbit/sec]



17. Does the ASSOCIATION RESPONSE indicate a Successful or Unsuccessful association response?

Status Code 的值决定了响应的成功与否。
如果状态码为 0，则表示成功关联。
若状态码为非零值，则表示关联尝试未成功，且该非零值通常对应于一个具体的错误代码，可以进一步查表了解详细的错误原因。



18. Does the fastest (largest) Extended Supported Rate the host has offered match the fastest (largest) Extended Supported Rate the AP is able to provide?

YES

结论：

1. 确定关联响应（ASSOCIATION RESPONSE）是否成功，“Status Code”这个字段的值决定了响应的成功与否。如果状态码为 0，则表示成功关联。若状态码为非零值，则表示关联尝试未成功，且该非零值通常对应于一个具体的错误代码，可以进一步查表了解详细的错误原因。
2. 802.11 层动作 - 解除关联请求：主机发送一个解除关联请求帧（Frame Type = 0，Subtype = 0xa）到 30 Munroe St AP。这是在 802.11 层面上直接执行的操作，用于告知 AP 主机打算断开当前的关联。
   802.11 层动作 - 解除关联响应：在 AP 接收到解除关联请求后，它会发送一个解除关联响应帧（Frame Type = 0，Subtype = 0xb）给主机，确认关联已被成功解除。这也是 802.11 层面上的操作，并非直接的 IP 层动作。
   IP 层动作可能是指后续可能发生的网络配置调整（如 DHCP RELEASE），但这并非直接关联于无线解关联过程本身。
3. 802.11 帧中的三个 MAC 地址字段分别是：
   源 MAC 地址（Source Address，SA）：表示帧的发送方 MAC 地址。
   目的 MAC 地址（Destination Address，DA）：表示帧的接收方 MAC 地址。
   BSSID（Basic Service Set Identifier）：在基础设施模式中，这通常与 AP 的 MAC 地址相同，标识了无线网络的基本服务集。