

**JARINGAN KOMPUTER – TUGAS PENDAHULUAN MODUL 14**  
**802.11 WI-FI PROTOCOL**

Nama : Muhammad Hamzah Haifan Ma'ruf

NIM : 2311102091

Kelas : S1IF-11-07

Kode Dosen : AIZ

**JAWABAN MODUL**

**A. Teori**

**1. Penjelasan tentang OSI Model dan TCP/IP Model beserta Protokolnya**

Model OSI (Open Systems Interconnection) terdiri dari tujuh lapisan yaitu Application, Presentation, Session, Transport, Network, Data Link, dan Physical. Sementara itu, model TCP/IP memiliki empat lapisan yaitu Application, Transport, Internet, dan Network Interface. Hubungan antara keduanya dapat digambarkan sebagai berikut: Lapisan Application pada TCP/IP mencakup tiga lapisan OSI, yaitu Application, Presentation, dan Session. Lapisan Transport tetap sama pada kedua model, dan lapisan Internet pada TCP/IP setara dengan lapisan Network pada OSI. Terakhir, lapisan Network Interface pada TCP/IP setara dengan kombinasi lapisan Data Link dan Physical pada OSI. Beberapa protokol dapat dikelompokkan berdasarkan lapisannya, seperti HTTP, FTP, SMTP, dan DNS yang berada di lapisan Application; TCP dan UDP pada lapisan Transport; IP dan ARP pada lapisan Network; serta Ethernet dan IEEE 802.11 (Wi-Fi) pada lapisan Data Link dan Physical. Protokol DHCP digunakan untuk memberikan alamat IP secara otomatis dan juga bekerja di lapisan Application serta melibatkan lapisan-lapisan bawah seperti Network dan Data Link.

**2. Penjelasan Gambar Figure 6.19 dan Cara Kerja IEEE 802.11 Wi-Fi**

Gambar Figure 6.19 menunjukkan dua subnet berbeda yang dihubungkan oleh sebuah router. Subnet pertama menggunakan rentang alamat IP 111.111.111.x,

sedangkan subnet kedua menggunakan 222.222.222.x. Masing-masing subnet terdiri dari beberapa komputer yang terhubung secara nirkabel menggunakan teknologi IEEE 802.11 Wi-Fi. Setiap perangkat memiliki IP address untuk identifikasi logis dan MAC address untuk identifikasi fisik di jaringan lokal. Dalam konteks pengiriman data antar subnet, misalnya komputer di subnet 111.111.111.x ingin mengirim data ke komputer di subnet 222.222.222.x, data akan dikirim melalui router. Prosesnya dimulai dari lapisan aplikasi, kemudian data dibungkus oleh protokol transport seperti TCP atau UDP, lalu diberikan alamat IP tujuan pada lapisan network. Karena tujuan berada di subnet berbeda, data dikirim ke router terlebih dahulu menggunakan MAC address router sebagai tujuan di lapisan data link. Router kemudian membaca IP tujuan, menentukan jalur menuju subnet 222.222.222.x, dan mengirimkan data melalui antarmuka Wi-Fi ke perangkat tujuan setelah menemukan MAC address-nya melalui protokol ARP. Dengan demikian, komunikasi antar subnet dapat berlangsung lancar meskipun menggunakan media nirkabel seperti Wi-Fi.

3. Perbedaan Arsitektur IEEE 802.11 LAN dan Penggunaan Field Alamat pada Frame IEEE 802.11

Gambar Figure 7.7 menunjukkan arsitektur dasar dari jaringan IEEE 802.11 LAN yang terdiri dari beberapa Basic Service Set (BSS), di mana setiap BSS memiliki sebuah Access Point (AP) yang menjadi pusat koneksi bagi perangkat client. Semua AP dalam gambar ini terhubung ke satu switch atau router, lalu menuju ke internet. Di sisi lain, gambar Figure 7.14 menjelaskan bagaimana field alamat digunakan dalam frame IEEE 802.11 saat pengiriman data, terutama ketika melibatkan perangkat client (misalnya H1) yang mengirim data ke router (R1) melalui AP. Perbedaan mendasar antara kedua gambar adalah bahwa Figure 7.7 menekankan struktur jaringan secara keseluruhan, sedangkan Figure 7.14 fokus pada proses pengalaman dan perpindahan data dalam frame saat melewati beberapa titik (client, AP, router).

Dalam kedua gambar tersebut, Access Point (AP) berfungsi sebagai jembatan nirkabel yang menghubungkan perangkat client ke jaringan kabel dan akhirnya ke internet. Setiap Basic Service Set (BSS) terdiri dari satu AP dan perangkat-perangkat client yang terhubung padanya secara langsung. Pada gambar Figure 7.7, setiap AP menangani lalu lintas dari perangkat-perangkat client di BSS-nya masing-masing, dan seluruh AP terhubung ke jaringan utama melalui switch atau router pusat. Sementara itu, pada gambar Figure 7.14, penekanan ada pada cara frame IEEE 802.11 membawa informasi alamat dengan menggunakan empat field

alamat: alamat pengirim (client), alamat penerima (router), alamat AP sebagai transmitter, dan alamat AP sebagai receiver jika diperlukan.

Router dalam kedua gambar bertindak sebagai penghubung antara jaringan lokal dan jaringan global (internet). Ia menerima data dari AP, membaca IP dan MAC address tujuan, lalu meneruskan ke jaringan luar atau ke subnet lain. Sedangkan perangkat client, seperti laptop atau ponsel, terhubung secara nirkabel ke AP dalam BSS masing-masing, mengirim dan menerima data melalui protokol 802.11.

Secara keseluruhan, meskipun kedua gambar sama-sama menunjukkan arsitektur jaringan berbasis IEEE 802.11, Figure 7.7 lebih bersifat topologis, menggambarkan bagaimana AP dan BSS saling terhubung dalam jaringan. Sementara itu, Figure 7.14 bersifat teknis, menjelaskan mekanisme pengalamatan frame saat data berpindah dari satu titik ke titik lain dalam jaringan Wi-Fi. Keduanya menyoroti pentingnya peran AP sebagai penghubung utama antara perangkat client dan jaringan kabel melalui router untuk memberikan akses internet.

#### 4. Penjelasan Pemindaian Aktif dan Pasif pada Wi-Fi serta Penggunaan Frame IEEE 802.11

Pada konteks Wi-Fi, terdapat dua metode utama yang digunakan perangkat untuk menemukan dan terhubung ke Access Point (AP), yaitu pemindaian pasif (passive scanning) dan pemindaian aktif (active scanning). Gambar Figure 7.9 menjelaskan kedua proses ini. Dalam pemindaian pasif, perangkat host seperti H1 menunggu sinyal beacon frame yang secara berkala dikirimkan oleh semua AP yang berada dalam jangkauan, seperti AP1 dan AP2 dalam gambar. Setelah menerima beacon frame, H1 memilih salah satu AP dan mengirimkan Association Request frame. Jika AP menerima permintaan tersebut, ia merespons dengan Association Response frame, menandakan bahwa H1 telah berhasil bergabung ke jaringan tersebut.

Sebaliknya, pada pemindaian aktif, H1 secara proaktif mengirimkan Probe Request frame yang disiarkan ke semua AP di sekitarnya. Setiap AP yang menerima permintaan ini akan mengirimkan kembali Probe Response frame. Setelah menerima tanggapan, H1 memilih salah satu AP, lalu mengirim Association Request, yang kemudian dibalas dengan Association Response oleh AP yang dipilih. Perbedaan utama antara kedua metode ini adalah bahwa pemindaian pasif lebih hemat daya karena host hanya menunggu sinyal, sedangkan pemindaian aktif lebih cepat tetapi lebih boros energi karena host mengirimkan broadcast.

Dalam kedua proses pemindaian ini, digunakan frame-frame khusus dari protokol IEEE 802.11, sebagaimana dijelaskan dalam Figure 7.13. Frame IEEE 802.11 terdiri dari berbagai field, di antaranya Frame Control, Duration, Address 1 hingga 4, Sequence Control, Payload, dan CRC. Field Frame Control terdiri dari subfield seperti type dan subtype yang menentukan jenis frame (misalnya, Management frame untuk beacon, probe, dan association), serta subfield lainnya seperti retry, power management, dan WEP (untuk enkripsi). Field Address 1 hingga 3 digunakan untuk menunjukkan MAC address sumber, tujuan, dan AP terkait, sedangkan Payload memuat informasi seperti SSID, kemampuan AP, dan informasi lainnya yang dibutuhkan untuk proses asosiasi.

Peran host (H1) dalam proses ini adalah sebagai client yang berusaha menemukan dan terhubung ke jaringan Wi-Fi. Access Point (AP) berperan menyediakan sinyal dan menjawab permintaan asosiasi. Proses scanning ini penting untuk membangun koneksi awal antara client dan jaringan Wi-Fi dengan cara yang efisien dan sesuai standar IEEE 802.11.

## B. Menggali Informasi dari Dokumen IEEE 802.11 Wi-Fi

### 1. Struktur Frame MAC IEEE 802.11 dan Fungsi Field-Fieldnya

Struktur frame MAC pada protokol IEEE 802.11 terdiri dari beberapa field penting yang menyusun format komunikasi pada jaringan nirkabel. Field utama meliputi Frame Control, Duration/ID, Address 1–4, Sequence Control, Frame Body, dan FCS (Frame Check Sequence). Field Frame Control menentukan jenis frame (data, control, atau management), subtype, serta status bit seperti To DS dan From DS. Field Duration/ID menentukan waktu alokasi medium. Empat address field digunakan tergantung arah komunikasi, seperti dari client ke AP atau antar-AP. Sequence Control menyusun urutan frame, sedangkan FCS mengecek kesalahan transmisi. Bit To DS dan From DS digunakan untuk menunjukkan arah data: apakah menuju distribution system (DS) atau berasal dari DS. Kombinasi bit ini penting untuk pengiriman data: misalnya, To DS = 1 dan From DS = 0 menunjukkan data dari client ke AP, sebaliknya To DS = 0 dan From DS = 1 berarti dari AP ke client.

## Frame Formats

All 802.11 frames are composed by the following components

Preamble	PLCP Header	MAC Data	CRC
----------	-------------	----------	-----

### Preamble

This is PHY dependent, and includes:

- **Synch:** An 80-bit sequence of alternating zeros and ones, which is used by the PHY circuitry to select the appropriate antenna (if diversity is used), and to reach steady-state frequency offset correction and synchronization with the received packet timing, and
- **SFD:** A Start Frame delimiter which consists of the 16-bit binary pattern 0000 1100 1011 1101, which is used to define the frame timing.

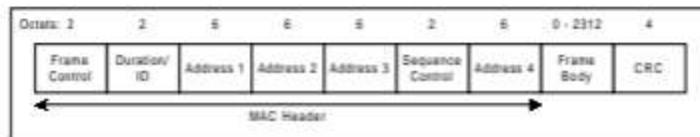
### PLCP Header

The PLCP Header is always transmitted at 1 Mbit/s and contains Logical information that will be used by the PHY Layer to decode the frame, and consists of:

- **PLCP\_PDU Length Word:** which represents the number of bytes contained in the packet, this is useful for the PHY to correctly detect the end of packet,
- **PLCP Signaling Field:** which currently contains only the rate information, encoded in 0.5 MBps increments from 1 Mbit/s to 4.5 Mbit/s, and
- **Header Error Check Field:** Which is a 16 Bit CRC error detection field

### MAC Data

The following figure shows the general MAC Frame Format, part of the fields are only present on part of the frames as described later.



halaman 16–17 Protocol IEEE 802.11.pdf

MEDIUM ACCESS CONTROL (MAC) AND PHYSICAL (PHY) SPECIFICATIONS ANSI/IEEE Std 802.11, 1999 Edition

DS. The DS uses this information to accomplish its message distribution service. How the information provided by the association service is stored and managed within the DS is not specified by this standard.

At any given instant, a STA may be associated with no more than one AP. This ensures that the DS may determine a unique answer to the question, "Which AP is serving STA X?" Once an association is completed, a STA may make full use of a DS (via the AP) to communicate. Association is always initiated by the mobile STA, not the AP.

An AP may be associated with many STAs at one time.

A STA learns what APs are present and then requests to establish an association by invoking the association service. For details of how a station learns about what APs are present, see 11.1.3.

#### 5.4.2.3 Reassociation

Association is sufficient for no-transition message delivery between IEEE 802.11 stations. Additional functionality is needed to support BSS-transition mobility. The additional required functionality is provided by the reassociation service. Reassociation is a DSS.

The reassociation service is invoked to "move" a current association from one AP to another. This keeps the DS informed of the current mapping between AP and STA as the station moves from BSS to BSS within an ESS. Reassociation also enables changing association attributes of an established association while the STA remains associated with the same AP. Reassociation is always initiated by the mobile STA.

#### 5.4.2.4 Disassociation

The disassociation service is invoked whenever an existing association is to be terminated. Disassociation is a DSS.

In an ESS, this tells the DS to void existing association information. Attempts to send messages via the DS to a disassociated STA will be unsuccessful.

The disassociation service may be invoked by either party to an association (non-AP STA or AP). Disassociation is a notification, not a request. Disassociation cannot be refused by either party to the association.

APs may need to disassociate STAs to enable the AP to be removed from a network for service or for other reasons.

STAs shall attempt to disassociate whenever they leave a network. However, the MAC protocol does not depend on STAs invoking the disassociation service. (MAC management is designed to accommodate loss of an associated STA.)

#### 5.4.3 Access and confidentiality control services

Two services are required for IEEE 802.11 to provide functionality equivalent to that which is inherent to wired LANs. The design of wired LANs assumes the physical attributes of wire. In particular, wired LAN design assumes the physically closed and controlled nature of wired media. The physically open medium nature of an IEEE 802.11 LAN violates those assumptions.

Two services are provided to bring the IEEE 802.11 functionality in line with wired LAN assumptions; authentication and privacy. Authentication is used instead of the wired media physical connection. Privacy is used to provide the confidential aspects of closed wired media.

*halaman 34–36 Dokumen Standar IEEE 802.11.pdf*

## 2. Enkapsulasi TCP/IP dalam Jaringan Wi-Fi dan Hubungan Alamat MAC–IP

Dalam jaringan Wi-Fi, data dari aplikasi dikemas secara bertingkat dari TCP, IP, hingga ke frame IEEE 802.11. Host wireless mengirim data menggunakan IP Address dan MAC Address-nya melalui Access Point (AP), yang meneruskan data ke router pertama (first-hop router). Alamat MAC digunakan untuk identifikasi perangkat secara fisik di jaringan lokal, sedangkan IP digunakan untuk

pengalamatan logis di jaringan global. Pada proses ini, MAC address pengirim adalah milik host, receiver adalah milik AP, dan alamat IP tujuan akan digunakan oleh router untuk routing lanjutan. Enkapsulasi mencakup pembungkusan segment TCP ke datagram IP, lalu ke frame MAC, hingga akhirnya dikirim melalui media wireless.

MEDIUM ACCESS CONTROL (MAC) AND PHYSICAL (PHY) SPECIFICATIONS ANSI/IEEE Std 802.11, 1999 Edition

DS. The DS uses this information to accomplish its message distribution service. How the information provided by the association service is stored and managed within the DS is not specified by this standard.

At any given instant, a STA may be associated with no more than one AP. This ensures that the DS may determine a unique answer to the question, "Which AP is serving STA X?" Once an association is completed, a STA may make full use of a DS (via the AP) to communicate. Association is always initiated by the mobile STA, not the AP.

An AP may be associated with many STAs at one time.

A STA learns what APs are present and then requests to establish an association by invoking the association service. For details of how a station learns about what APs are present, see 11.1.3.

#### 5.4.2.3 Reassociation

Association is sufficient for no-transition message delivery between IEEE 802.11 stations. Additional functionality is needed to support BSS-transition mobility. The additional required functionality is provided by the reassociation service. Reassociation is a DSS.

The reassociation service is invoked to "move" a current association from one AP to another. This keeps the DS informed of the current mapping between AP and STA as the station moves from BSS to BSS within an ESS. Reassociation also enables changing association attributes of an established association while the STA remains associated with the same AP. Reassociation is always initiated by the mobile STA.

#### 5.4.2.4 Disassociation

The disassociation service is invoked whenever an existing association is to be terminated. Disassociation is a DSS.

In an ESS, this tells the DS to void existing association information. Attempts to send messages via the DS to a disassociated STA will be unsuccessful.

The disassociation service may be invoked by either party to an association (non-AP STA or AP). Disassociation is a notification, not a request. Disassociation cannot be refused by either party to the association.

APs may need to disassociate STAs to enable the AP to be removed from a network for service or for other reasons.

STAs shall attempt to disassociate whenever they leave a network. However, the MAC protocol does not depend on STAs invoking the disassociation service. (MAC management is designed to accommodate loss of an associated STA.)

#### 5.4.3 Access and confidentiality control services

Two services are required for IEEE 802.11 to provide functionality equivalent to that which is inherent to wired LANs. The design of wired LANs assumes the physical attributes of wire. In particular, wired LAN design assumes the physically closed and controlled nature of wired media. The physically open medium nature of an IEEE 802.11 LAN violates those assumptions.

Two services are provided to bring the IEEE 802.11 functionality in line with wired LAN assumptions; authentication and privacy. Authentication is used instead of the wired media physical connection. Privacy is used to provide the confidential aspects of closed wired media.

*halaman 34–58 Dokumen Standar IEEE 802.11.pdf*

3. Informasi yang Dibawa dalam Beacon Frame

Beacon frame adalah salah satu jenis frame manajemen dalam IEEE 802.11 yang dikirim secara periodik oleh AP untuk mengumumkan keberadaan jaringan nirkabelnya. SSID (Service Set Identifier) menunjukkan nama jaringan, sementara interval pengiriman beacon biasanya 100 TU (1 TU = 1.024 mikrodetik). Dalam beacon frame, alamat MAC source adalah milik AP, destination address adalah alamat broadcast (FF:FF:FF:FF:FF), dan BSS ID juga adalah MAC dari AP itu sendiri. Selain itu, beacon frame memuat Supported Rates dan Extended Supported Rates, yaitu kecepatan transmisi data yang bisa digunakan klien saat terkoneksi dengan AP tersebut.

MEDIUM ACCESS CONTROL (MAC) AND PHYSICAL (PHY) SPECIFICATIONS ANSI/IEEE Std 802.11, 1999 Edition

```
dot11MulticastTransmittedFrameCount OBJECT-TYPE
  SYNTAX Counter32
  MAX-ACCESS read-only
  STATUS current
  DESCRIPTION
    "This counter shall increment only when the multicast
    bit is set in the destination MAC address of a successfully
    transmitted MSDU. When operating as a STA in an ESS, where
    these frames are directed to the AP, this implies having
    received an acknowledgment to all associated MSDUs."
 ::= { dot11CountersEntry 2 }

dot11FailedCount OBJECT-TYPE
  SYNTAX Counter32
  MAX-ACCESS read-only
  STATUS current
  DESCRIPTION
    "This counter shall increment when an MSDU is not
    transmitted successfully due to the number of
    transmit attempts exceeding either the
    dot11ShortRetryLimit or dot11LongRetryLimit."
 ::= { dot11CountersEntry 3 }

dot11RetryCount OBJECT-TYPE
  SYNTAX Counter32
  MAX-ACCESS read-only
  STATUS current
  DESCRIPTION
    "This counter shall increment when an MSDU is successfully
    transmitted after one or more retransmissions."
 ::= { dot11CountersEntry 4 }

dot11MultipleRetryCount OBJECT-TYPE
  SYNTAX Counter32
  MAX-ACCESS read-only
  STATUS current
  DESCRIPTION
    "This counter shall increment when an MSDU is successfully
    transmitted after more than one retransmission."
 ::= { dot11CountersEntry 5 }

dot11FrameDuplicateCount OBJECT-TYPE
  SYNTAX Counter32
  MAX-ACCESS read-only
  STATUS current
  DESCRIPTION
    "This counter shall increment when a frame is received
    that the Sequence Control field indicates is a
    duplicate."
 ::= { dot11CountersEntry 6 }
```

Copyright © 1999 IEEE. All rights reserved.

487

halaman 497–500 Dokumen Standar IEEE 802.11.pdf

#### 5.1.1.4 Interaction with other IEEE 802 layers

IEEE 802.11 is required to appear to higher layers [logical link control (LLC)] as a current style IEEE 802 LAN. This requires that the IEEE 802.11 network handle station mobility within the MAC sublayer. To meet reliability assumptions (that LLC makes about lower layers), it is necessary for IEEE 802.11 to incorporate functionality that is untraditional for MAC sublayers.

### 5.2 Components of the IEEE 802.11 architecture

The IEEE 802.11 architecture consists of several components that interact to provide a wireless LAN that supports station mobility transparently to upper layers.

The basic service set (BSS) is the basic building block of an IEEE 802.11 LAN. Figure 1 shows two BSSs, each of which has two stations that are members of the BSS.

It is useful to think of the ovals used to depict a BSS as the coverage area within which the member stations of the BSS may remain in communication. (The concept of area, while not precise, is often good enough.) If a station moves out of its BSS, it can no longer directly communicate with other members of the BSS.

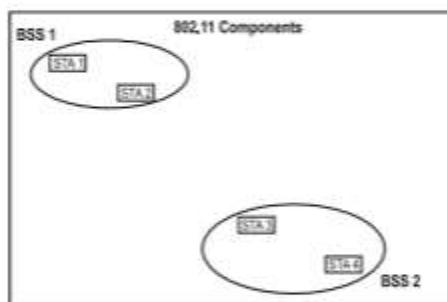


Figure 1—Basic service sets

#### 5.2.1 The independent BSS as an ad hoc network

The independent BSS (IBSS) is the most basic type of IEEE 802.11 LAN. A minimum IEEE 802.11 LAN may consist of only two stations.

Figure 1 shows two IBSSs. This mode of operation is possible when IEEE 802.11 stations are able to communicate directly. Because this type of IEEE 802.11 LAN is often formed without pre-planning, for only as long as the LAN is needed, this type of operation is often referred to as an *ad hoc network*.

##### 5.2.1.1 STA to BSS association is dynamic

The association between a STA and a BSS is dynamic (STAs turn on, turn off, come within range, and go out of range). To become a member of an infrastructure BSS, a station shall become "associated." These associations are dynamic and involve the use of the distribution system service (DSS), which is described in 5.3.2.

## 4. Tahap Autentikasi dan Asosiasi pada IEEE 802.11

Sebelum klien (host) dapat terhubung ke jaringan WiFi, ia harus melalui tahap authentication dan association. Protokol IEEE 802.11 secara default menggunakan metode Open System Authentication, namun juga mendukung Shared Key Authentication menggunakan kunci WEP. Setelah autentikasi berhasil, klien

mengirimkan Association Request, yang kemudian dibalas oleh AP dengan Association Response. Frame tersebut memuat parameter penting seperti Supported Rates, Capability Info, serta Challenge Text (jika menggunakan shared key). Keberhasilan kedua tahap ini menandai bahwa klien telah resmi menjadi bagian dari jaringan BSS dan bisa berkomunikasi melalui AP

```

MEDIUM ACCESS CONTROL (MAC) AND PHYSICAL (PHY) SPECIFICATIONS ANSI/IEEE Std 802.11, 1999 Edition

dot11MulticastTransmittedFrameCount OBJECT-TYPE
  SYNTAX Counter32
  MAX-ACCESS read-only
  STATUS current
  DESCRIPTION
    "This counter shall increment only when the multicast
    bit is set in the destination MAC address of a successfully
    transmitted MSDU. When operating as a STA in an ESS, where
    these frames are directed to the AP, this implies having
    received an acknowledgement to all associated MSDUs."
 ::= { dot11CountersEntry 2 }

dot11FailedCount OBJECT-TYPE
  SYNTAX Counter32
  MAX-ACCESS read-only
  STATUS current
  DESCRIPTION
    "This counter shall increment when an MSDU is not
    transmitted successfully due to the number of
    transmit attempts exceeding either the
    dot11ShortRetryLimit or dot11LongRetryLimit."
 ::= { dot11CountersEntry 3 }

dot11RetryCount OBJECT-TYPE
  SYNTAX Counter32
  MAX-ACCESS read-only
  STATUS current
  DESCRIPTION
    "This counter shall increment when an MSDU is successfully
    transmitted after one or more retransmissions."
 ::= { dot11CountersEntry 4 }

dot11MultipleRetryCount OBJECT-TYPE
  SYNTAX Counter32
  MAX-ACCESS read-only
  STATUS current
  DESCRIPTION
    "This counter shall increment when an MSDU is successfully
    transmitted after more than one retransmission."
 ::= { dot11CountersEntry 5 }

dot11FrameDuplicateCount OBJECT-TYPE
  SYNTAX Counter32
  MAX-ACCESS read-only
  STATUS current
  DESCRIPTION
    "This counter shall increment when a frame is received
    that the Sequence Control field indicates is a
    duplicate."
 ::= { dot11CountersEntry 6 }

```

## 5. Interaksi Alamat MAC dan IP Saat Pengiriman Data

Dalam pengiriman data melalui jaringan WiFi, AP berfungsi sebagai jembatan antara jaringan lokal (wireless) dan jaringan luar (wired). AP menggunakan alamat MAC untuk menentukan perangkat penerima dalam jaringan lokal, sedangkan IP digunakan untuk menentukan jalur pada jaringan lebih luas. Saat data dikirim, alamat MAC tujuan dalam frame bukanlah alamat IP tujuan akhir, melainkan alamat perangkat fisik terdekat (misalnya router pertama). Dengan demikian, alamat MAC dalam frame 802.11 tidak selalu sama dengan alamat IP tujuan. Proses ini didukung dengan mekanisme ARP (Address Resolution Protocol) untuk mencocokkan IP dan MAC, serta NAT pada sisi router untuk komunikasi ke luar jaringan.

## 7. Frame formats

The format of the MAC frames is specified in this clause. All stations shall be able to properly construct frames for transmission and decode frames upon reception, as specified in this clause.

### 7.1 MAC frame formats

Each frame consists of the following basic components:

- a) A *MAC header*, which comprises frame control, duration, address, and sequence control information;
- b) A variable length *frame body*, which contains information specific to the frame type;
- c) A *frame check sequence* (FCS), which contains an IEEE 32-bit cyclic redundancy code (CRC).

#### 7.1.1 Conventions

The MAC protocol data units (MPDUs) or frames in the MAC sublayer are described as a sequence of fields in specific order. Each figure in Clause 7 depicts the fields/subfields as they appear in the MAC frame and in the order in which they are passed to the physical layer convergence protocol (PLCP), from left to right.

In figures, all bits within fields are numbered, from 0 to  $k$ , where the length of the field is  $k + 1$  bit. The octet boundaries within a field can be obtained by taking the bit numbers of the field modulo 8. Octets within numeric fields that are longer than a single octet are depicted in increasing order of significance, from lowest numbered bit to highest numbered bit. The octets in fields longer than a single octet are sent to the PLCP in order from the octet containing the lowest numbered bits to the octet containing the highest numbered bits.

Any field containing a CRC is an exception to this convention and is transmitted commencing with the coefficient of the highest-order term.

MAC addresses are assigned as ordered sequences of bits. The Individual/Group bit is always transferred first and is bit 0 of the first octet.

Values specified in decimal are coded in natural binary unless otherwise stated. The values in Table 1 are in binary, with the bit assignments shown in the table. Values in other tables are shown in decimal notation.

Reserved fields and subfields are set to 0 upon transmission and are ignored upon reception.

#### 7.1.2 General frame format

The MAC frame format comprises a set of fields that occur in a fixed order in all frames. Figure 12 depicts the general MAC frame format. The fields Address 2, Address 3, Sequence Control, Address 4, and Frame Body are only present in certain frame types. Each field is defined in 7.1.3. The format of each of the individual frame types is defined in 7.2.



Figure 12—MAC frame format

## 6. Perbedaan Passive dan Active Scanning serta Penggunaan Frame Probe

Dalam proses pencarian jaringan WiFi, klien dapat menggunakan dua metode scanning: passive dan active. Pada passive scanning, host hanya menunggu dan menerima beacon dari AP. Sedangkan pada active scanning, host mengirimkan Probe Request ke semua AP terdekat. AP yang menerima akan membalas dengan

Probe Response. Klien memilih AP berdasarkan informasi dalam Probe Response seperti SSID, signal strength, dan Supported Rates. Dalam frame Probe Request, MAC sender adalah host, receiver biasanya adalah broadcast atau AP tertentu, dan BSS ID diisi dengan null atau SSID spesifik. Pada Probe Response, MAC sender adalah AP, receiver adalah MAC host, dan BSS ID adalah MAC dari AP.

### IEEE 802.11 Architecture

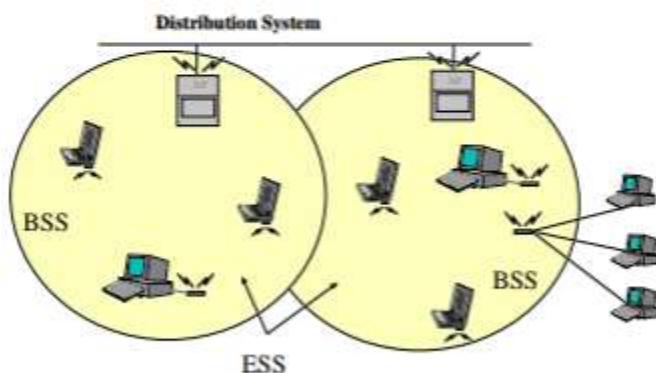
#### Architecture Components

An 802.11 LAN is based on a cellular architecture where the system is subdivided into cells, where each cell (called Basic Service Set or BSS, in the 802.11 nomenclature) is controlled by a Base Station (called Access Point, or in short AP).

Even though that a wireless LAN may be formed by a single cell, with a single Access Point, (and as will be described later, it can also work without an Access Point), most installations will be formed by several cells, where the Access Points are connected through some kind of backbone (called Distribution System or DS), typically Ethernet, and in some cases wireless itself.

The whole interconnected Wireless LAN including the different cells, their respective Access Points and the Distribution System, is seen to the upper layers of the OSI model, as a single 802 network, and is called in the Standard as **Extended Service Set (ESS)**.

The following picture shows a typical 802.11 LAN, with the components described previously:



The standard also defines the concept of a **Portal**, a Portal is a device that interconnects between an 802.11 and another 802 LAN. This concept is an abstract description of part of the functionality of a "translation bridge".

*halaman 1 Protocol IEEE 802.11.pdf*

MEDIUM ACCESS CONTROL (MAC) AND PHYSICAL (PHY) SPECIFICATIONS ANSI/IEEE Std 802.11, 1999 Edition

```

DESCRIPTION
    "The transmit output power for LEVEL6 in mW."
 ::= { dot11PhyTxPowerEntry 7 }

dot11TxPowerLevel7 OBJECT-TYPE
    SYNTAX INTEGER (0..10000)
    MAX-ACCESS read-only
    STATUS current
    DESCRIPTION
        "The transmit output power for LEVEL7 in mW."
 ::= { dot11PhyTxPowerEntry 8 }

dot11TxPowerLevel8 OBJECT-TYPE
    SYNTAX INTEGER (0..10000)
    MAX-ACCESS read-only
    STATUS current
    DESCRIPTION
        "The transmit output power for LEVEL8 in mW."
 ::= { dot11PhyTxPowerEntry 9 }

dot11CurrentTxPowerLevel OBJECT-TYPE
    SYNTAX INTEGER (1..8)
    MAX-ACCESS read-write
    STATUS current
    DESCRIPTION
        "The TxPowerLevel is currently being used to transmit data.
        Some Piffs also use this value to determine the receiver
        sensitivity requirements for CCA."
 ::= { dot11PhyTxPowerEntry 10 }

-- *****
-- * End of dot11PhyTxPower TABLE
-- *****

-- *****
-- * dot11PhyFREQS TABLE
-- *****
dot11PhyFREQSTable OBJECT-TYPE
    SYNTAX SEQUENCE OF dot11PhyFREQSentry
    MAX-ACCESS not-accessible
    STATUS current
    DESCRIPTION
        "Group of attributes for dot11PhyFREQSTable. Implemented as a
        table indexed on STA ID to allow for multiple instances on
        an Agent."
 ::= { dot11Phy 4 }

dot11PhyFREQSentry OBJECT-TYPE
    SYNTAX Dot11PhyFREQSentry
    MAX-ACCESS not-accessible
    STATUS current
    DESCRIPTION
        "An entry in the dot11PhyFREQS Table.

        ifIndex - Each 802.11 interface is represented by an
        ifIndex. Interface tables in this MIB module are indexed
        by ifIndex."

```

Copyright © 1999 IEEE. All rights reserved.

497

*halaman 497 Dokumen Standar IEEE 802.11.pdf*

ANSI/IEEE Std 802.11, 1999 Edition

LOCAL AND METROPOLITAN AREA NETWORKS: WIRELESS LAN

#### 5.1.1.4 Interaction with other IEEE 802 layers

IEEE 802.11 is required to appear to higher layers [logical link control (LLC)] as a current style IEEE 802 LAN. This requires that the IEEE 802.11 network handle station mobility within the MAC sublayer. To meet reliability assumptions (that LLC makes about lower layers), it is necessary for IEEE 802.11 to incorporate functionality that is untraditional for MAC sublayers.

#### 5.2 Components of the IEEE 802.11 architecture

The IEEE 802.11 architecture consists of several components that interact to provide a wireless LAN that supports station mobility transparently to upper layers.

The basic service set (BSS) is the basic building block of an IEEE 802.11 LAN. Figure 1 shows two BSSs, each of which has two stations that are members of the BSS.

It is useful to think of the ovals used to depict a BSS as the coverage area within which the member stations of the BSS may remain in communication. (The concept of area, while not precise, is often good enough.) If a station moves out of its BSS, it can no longer directly communicate with other members of the BSS.

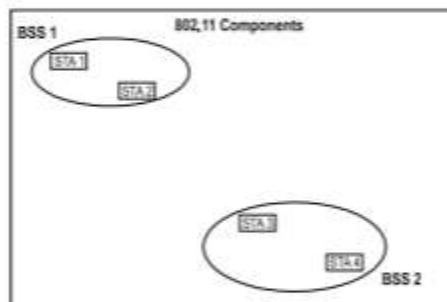


Figure 1—Basic service sets

##### 5.2.1 The independent BSS as an ad hoc network

The independent BSS (IBSS) is the most basic type of IEEE 802.11 LAN. A minimum IEEE 802.11 LAN may consist of only two stations.

Figure 1 shows two IBSSs. This mode of operation is possible when IEEE 802.11 stations are able to communicate directly. Because this type of IEEE 802.11 LAN is often formed without pre-planning, for only as long as the LAN is needed, this type of operation is often referred to as an *ad hoc network*.

###### 5.2.1.1 STA to BSS association is dynamic

The association between a STA and a BSS is dynamic (STAs turn on, turn off, come within range, and go out of range). To become a member of an infrastructure BSS, a station shall become "associated." These associations are dynamic and involve the use of the distribution system service (DSS), which is described in 5.3.2.

## C. Wireshark 802.11 Wi-Fi

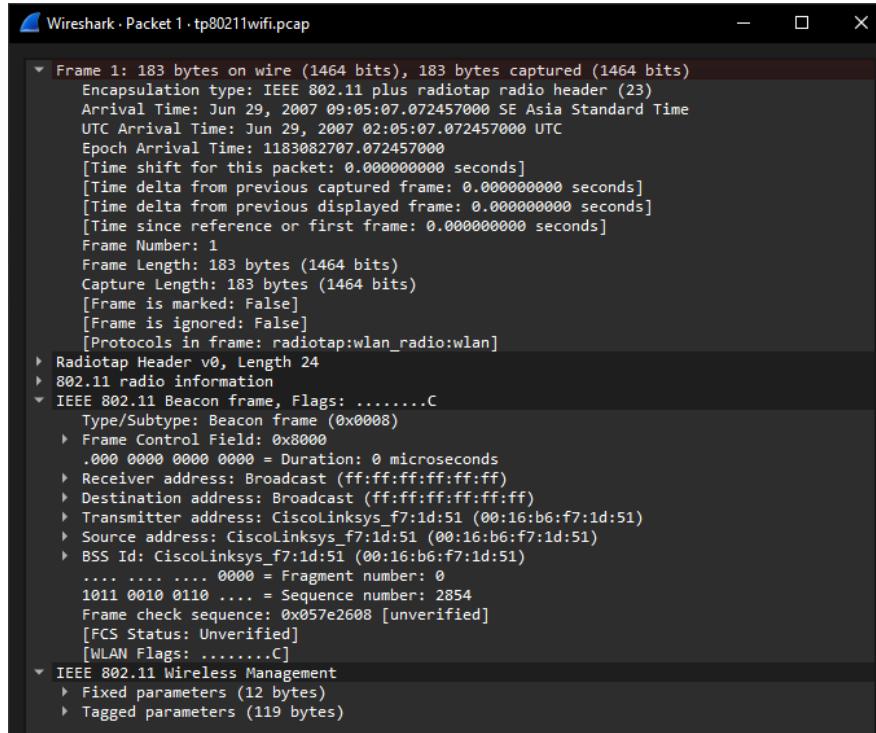
### 1. Analisis Struktur Beacon Frame

Beacon frame adalah salah satu jenis management frame dalam protokol IEEE 802.11 yang digunakan oleh Access Point (AP) untuk mengumumkan

keberadaannya kepada perangkat nirkabel di sekitarnya. Pada frame nomor 1, informasi penting dari struktur frame WiFi dapat dijelaskan sebagai berikut:

- Frame Control Field (0x8000): Menunjukkan bahwa frame ini adalah beacon frame (type: Management, subtype: 8).
- Source Address: 00:16:b6:f7:1d:51 — Ini adalah MAC Address dari Access Point yang mengirimkan beacon.
- Transmitter Address dan BSS ID: Juga 00:16:b6:f7:1d:51, menandakan bahwa AP ini juga merupakan basis dari jaringan tersebut.
- Receiver Address dan Destination Address: ff:ff:ff:ff:ff:ff — Ini adalah alamat broadcast, karena beacon dikirim ke semua perangkat dalam jangkauan.
- Sequence Number: 2854 — Menunjukkan urutan beacon yang dikirimkan oleh AP ini, digunakan untuk sinkronisasi dan manajemen lalu lintas.
- SSID (terdapat di bagian Tagged Parameters): Untuk melihat SSID lengkap, perlu dibuka bagian Tagged Parameters yang mencantumkan nama jaringan WiFi yang diumumkan.

Beacon frame ini membantu perangkat mengetahui adanya jaringan WiFi dan memulai proses koneksi seperti autentikasi dan asosiasi.



## 2. Analisis Interaksi HTTP dengan MAC Intel\_d1:b6:4f

IP Source: 192.168.1.109

IP Destination: 128.119.245.12

Port:

- Klien: port acak (>1024)
- Server: port 80 (HTTP)

Jenis HTTP Response:

- HTTP/1.1 200 OK (permintaan berhasil)
- HTTP/1.1 404 Not Found (tidak ditemukan)
- Tipe Frame Wi-Fi (802.11):
  - Frame Data
  - Source MAC: Intel\_d1:b6:4f
  - Destination MAC: alamat AP/router

Kesimpulan:

Perangkat dengan MAC Intel\_d1:b6:4f meminta file /wireshark-labs/alice.txt dari server 128.119.245.12 dan mendapatkan respons HTTP 200 OK.

No.	Time	Source	Destination	Protocol	length	Info
480 24.852953	192.168.1.109	128.119.245.12	HTTP	517	GET /wireshark-labs/alice.txt HTTP/1.1	
868 25.126724	128.119.245.12	192.168.1.109	HTTP	488	HTTP/1.1 200 OK (text/plain)[Illegal Segments]	
873 25.185581	192.168.1.109	128.119.245.12	HTTP	444	GET /favicon.ico HTTP/1.1	
875 25.189248	128.119.245.12	192.168.1.109	HTTP/0.9	1527	HTTP/1.1 404 Not Found	
1016 32.825992	192.168.1.109	128.119.240.19	HTTP	512	GET / HTTP/1.1	
1059 32.892294	192.168.1.109	128.119.240.19	HTTP	484	GET /includes/cowrie.css HTTP/1.1	
1062 32.940267	192.168.1.109	128.119.101.5	HTTP	469	GET /favicon.ico HTTP/1.1	
1066 32.500945	128.119.240.19	192.168.1.109	HTTP	464	HTTP/1.1 200 OK (text/html)	
1098 32.939781	128.119.240.19	192.168.1.109	HTTP	353	HTTP/1.1 200 OK (text/css)[Illegal Segments]	
1110 32.946609	128.119.101.5	192.168.1.109	HTTP	753	HTTP/1.1 200 OK (image/x-icon)[Illegal Segments]	
1117 32.956076	192.168.1.109	128.119.101.5	HTTP	586	GET /www/identity/b6p_strip/w_forsal_lgrey.gif	
1129 32.977290	128.119.101.5	192.168.1.109	HTTP	149	HTTP/1.1 200 OK (GIF89a)	
1140 32.500813	192.168.1.109	128.119.240.19	HTTP	484	GET /images/spacer.gif HTTP/1.1	
1169 33.022167	192.168.1.109	128.119.240.19	HTTP	489	GET /images/slide_entrance.jpg HTTP/1.1	
1183 33.032812	192.168.1.109	64.233.187.184	HTTP	488	GET /archin.js HTTP/1.1	
1254 33.409558	128.119.240.19	192.168.1.109	HTTP	188	HTTP/1.1 200 OK (GIF89a)	
1274 33.114482	128.119.240.19	192.168.1.109	HTTP	1336	HTTP/1.1 200 OK (JPEG-JFIF-Image)	
1289 33.122283	192.168.1.109	128.119.240.19	HTTP	489	GET /images/moonrise.gif HTTP/1.1	
1298 33.138796	64.233.187.184	192.168.1.109	HTTP	646	HTTP/1.1 200 OK (text/javascript)	
1385 33.148393	192.168.1.109	128.119.240.19	HTTP	485	GET /Images/cralogon.gif HTTP/1.1	
1389 33.146128	128.119.240.19	192.168.1.109	HTTP	393	HTTP/1.1 200 OK (GIF89a)	
1325 33.103626	128.119.240.19	192.168.1.109	HTTP	1258	HTTP/1.1 200 OK (GIF89a)	
1333 33.167722	192.168.1.109	64.231.187.104	HTTP	946	GET /_vtw.gif?vtbewv!&utam=1588792852&utmc=150-885	
1398 33.214655	64.233.187.104	192.168.1.109	HTTP	431	HTTP/1.1 200 OK (GIF89a)	

### 3. Analisis Beacon Frames dan SSID

SSID dari AP yang paling sering muncul:

Dari screenshot terlihat SSID CiscoLinksys\_F7:1d sering muncul sebagai Source Address.

Beacon Interval Rata-rata:

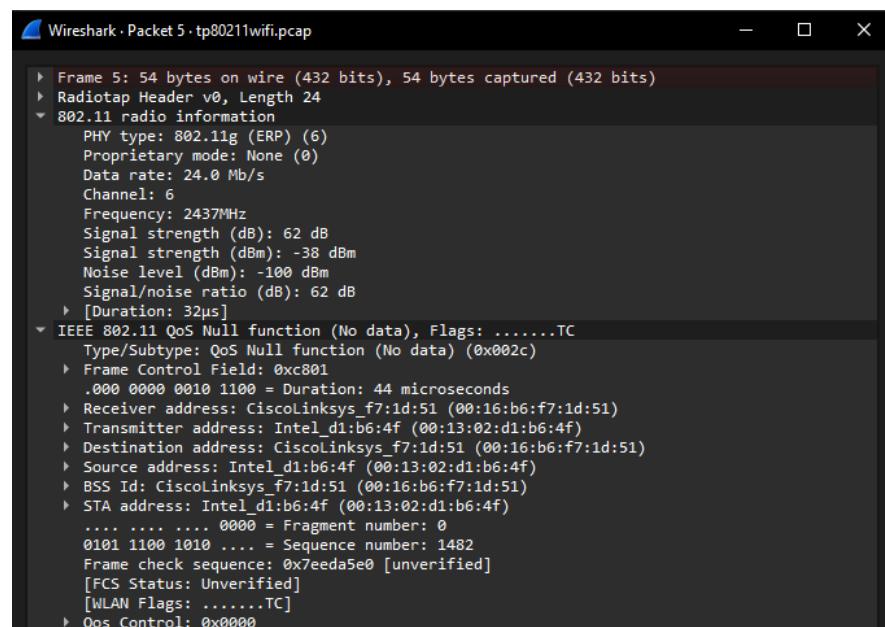
Beacon Interval biasanya diatur oleh AP, umumnya 100 TU (Time Unit) = 102,4 ms. Dari daftar, frame Beacon ini muncul secara berurutan dengan jeda waktu yang konsisten mendekati 0,1 detik (100 ms).

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	CiscoLinksys_f7:1d:51	Broadcast	802.11	183	Beacon Frame, S=M=0254, P=0+0, Flags=.....C,
2	0.005474	CiscoLinksys_f7:1d:51	Broadcast	802.11	183	Beacon Frame, S=M=0255, P=0+0, Flags=.....C,
4	0.187919	CiscoLinksys_f7:1d:51	Broadcast	802.11	183	Beacon Frame, S=M=0256, P=0+0, Flags=.....C,
9	0.294834	CiscoLinksys_f7:1d:51	Broadcast	802.11	183	Beacon Frame, S=M=0257, P=0+0, Flags=.....C,
10	0.294832	LinksysGroup_67:22:11	Broadcast	802.11	98	Beacon Frame, S=M=0272, P=0+0, Flags=.....C,
11	0.395374	CiscoLinksys_f7:1d:51	Broadcast	802.11	183	Beacon Frame, S=M=0258, P=0+0, Flags=.....C,
13	0.495632	CiscoLinksys_f7:1d:51	Broadcast	802.11	183	Beacon Frame, S=M=0259, P=0+0, Flags=.....C,
14	0.495937	LinksysGroup_67:22:11	Broadcast	802.11	98	Beacon Frame, S=M=0274, P=0+0, Flags=.....C,
15	0.597382	CiscoLinksys_f7:1d:51	Broadcast	802.11	183	Beacon Frame, S=M=0260, P=0+0, Flags=.....C,
16	0.601687	LinksysGroup_67:22:11	Broadcast	802.11	98	Beacon Frame, S=M=0275, P=0+0, Flags=.....C,
17	0.659647	CiscoLinksys_f7:1d:51	Broadcast	802.11	183	Beacon Frame, S=M=0261, P=0+0, Flags=.....C,
18	0.860228	CiscoLinksys_f7:1d:51	Broadcast	802.11	183	Beacon Frame, S=M=0282, P=0+0, Flags=.....C,
19	0.984619	CiscoLinksys_f7:1d:51	Broadcast	802.11	183	Beacon Frame, S=M=0283, P=0+0, Flags=.....C,
20	1.097015	CiscoLinksys_f7:1d:51	Broadcast	802.11	183	Beacon Frame, S=M=0284, P=0+0, Flags=.....C,
21	1.439949	LinksysGroup_67:22:11	Broadcast	802.11	98	Beacon Frame, S=M=0279, P=0+0, Flags=.....C,
22	1.586986	CiscoLinksys_f7:1d:51	Broadcast	802.11	183	Beacon Frame, S=M=0285, P=0+0, Flags=.....C,
23	1.533692	LinksysGroup_67:22:11	Broadcast	802.11	98	Beacon Frame, S=M=0288, P=0+0, Flags=.....C,
24	1.211043	CiscoLinksys_f7:1d:51	Broadcast	802.11	183	Beacon Frame, S=M=0286, P=0+0, Flags=.....C,
25	1.235947	LinksysGroup_67:22:11	Broadcast	802.11	98	Beacon Frame, S=M=0281, P=0+0, Flags=.....C,
26	1.534223	CiscoLinksys_f7:1d:51	Broadcast	802.11	183	Beacon Frame, S=M=0289, P=0+0, Flags=.....C,
27	1.436593	CiscoLinksys_f7:1d:51	Broadcast	802.11	183	Beacon Frame, S=M=0280, P=0+0, Flags=.....C,
28	1.426555	LinksysGroup_67:22:11	Broadcast	802.11	98	Beacon Frame, S=M=0285, P=0+0, Flags=.....C,
29	1.532999	CiscoLinksys_f7:1d:51	Broadcast	802.11	183	Beacon Frame, S=M=0276, P=0+0, Flags=.....C,
30	1.621402	CiscoLinksys_f7:1d:51	Broadcast	802.11	183	Beacon Frame, S=M=0287, P=0+0, Flags=.....C,
31	1.730071	CiscoLinksys_f7:1d:51	Broadcast	802.11	183	Beacon Frame, S=M=0277, P=0+0, Flags=.....C,
32	1.380103	CiscoLinksys_f7:1d:51	Broadcast	802.11	183	Beacon Frame, S=M=0275, P=0+0, Flags=.....C,
33	1.932099	CiscoLinksys_f7:1d:51	Broadcast	802.11	183	Beacon Frame, S=M=0274, P=0+0, Flags=.....C,
34	2.050007	CiscoLinksys_f7:1d:51	Broadcast	802.11	183	Beacon Frame, S=M=0275, P=0+0, Flags=.....C,

#### 4. Apakah Perangkat Intel\_d1:b6:4f Melakukan Authentication & Association?

Terlihat frame QoS Null Function (No data), bukan Authentication atau Association.

Tidak ada tanda-tanda Authentication Request/Response (0x000b/0x000c) atau Association Request/Response (0x0000/0x0001) untuk perangkat Intel\_d1:b6:4f.



## 5. Apakah Ada Indikasi Discovery Jaringan?

Terlihat adanya Probe Response dari AP dengan SSID CiscoLinksys\_f7:1d ditujukan ke perangkat Intel\_d1:b6:4f. Ini menandakan adanya discovery jaringan Wi-Fi, di mana perangkat melakukan scan SSID dan menerima tanggapan dari AP.

