**ĐẠI HỌC QUỐC GIA TP.HỒ CHÍ MINH**

TRƯỜNG ĐẠI HỌC BÁCH KHOA

o0o



**BÁO CÁO BÀI TẬP LỚN MÔN HỌC MẠNG MÁY TÍNH LỚP L01 – NHÓM 7**

**Giảng viên: Nguyễn Chí Ngọc**

**ĐỀ TÀI:**

**DATALINK LAYER**

**Danh sách thành viên:**

|  |  |  |
| --- | --- | --- |
| **STT** | **Họ và tên** | **MSSV** |
| **1** | **Mai Thành Danh** | **1910907** |
| **2** | **Lê Hà Đăng** | **1911036** |
| **3** | **Nguyễn Đức Huy** | **1911242** |
| **4** | **Lương Văn Long** | **1911514** |
| **5** | **Bùi Đình Phú** | **1911843** |

*TPHCM, tháng 9 năm 2022*

DANH MỤC HÌNH ẢNH

[Hình 1. Các thành phần mạng Ethernet. 8](#_bookmark5)

[Hình 2. Cách đọc tên các chuẩn Ethernet. 9](#_bookmark7)

[Hình 3. Ethernet II frame 13](#_bookmark9)

[Hình 4. IEEE 802.3 frame. 13](#_bookmark10)

[Hình 5. IEEE 802.3 frame có thêm SNAP 13](#_bookmark11)

[Hình 6. Cấu trúc khung của ethernet 13](#_bookmark12)

[Hình 7. Các thiết bị kết nối mạng WLAN. 15](#_bookmark16)

[Hình 8. Mô hình liên kết mạng WLAN. 16](#_bookmark18)

[Hình 9. Hệ thống WLAN cho phép thiết bị kết nối mạng nhanh chóng. 18](#_bookmark21)

[Hình 10. Mạng WLAN tồn tại nhược điểm về tính bảo mật. 19](#_bookmark22)

[Hình 11. Mô hình Access Point. 21](#_bookmark24)

[Hình 12. Card PCI Wireless. 21](#_bookmark25)

[Hình 13. Mô hình mạng Repeater. 22](#_bookmark27)

[Hình 14. Mô hình mạng Workgroup bridge. 23](#_bookmark28)

[Hình 15. Mô hình mạng Mesh. 23](#_bookmark29)

[Hình 16. Cấu trúc khung của Frame relay. 31](#_bookmark35)

[Hình 17. Cấu trúc trường Address. 31](#_bookmark36)

[Hình 18. Topology của mạng mô phỏng 34](#_bookmark41)

[Hình 19. Gói tin bắt đầu từ PC Giam doc: Mô hình OSI. 35](#_bookmark42)

[Hình 20. Gói tin bắt đầu từ PC Giam doc: Dạng khung dữ liệu. 35](#_bookmark43)

[Hình 21. Gói tin được gửi đến Switch. 36](#_bookmark44)

[Hình 22. Gói tin phản hồi từ PC Thu Ky: Mô hình OSI 36](#_bookmark45)

[Hình 23. Gói tin phản hồi từ PC Thu Ky: Dạng khung dữ liệu. 37](#_bookmark46)

[Hình 24. Ping từ Laptop0 đến Laptop3 37](#_bookmark48)

[Hình 25. Gói tin chuẩn bị gửi từ Laptop0. 38](#_bookmark49)

[Hình 26. Gói tin ở Wireless Router. 39](#_bookmark50)

[Hình 27. Gói tin phản hồi lại Laptop0 40](#_bookmark51)

[Hình 28. Mô hình mạng mô phỏng Frame Relay. 40](#_bookmark53)

[Hình 29. Gói tin ở PC0 chuẩn bị được gửi đi: Mô hình OSI. 41](#_bookmark54)

[Hình 30. Gói tin ở PC0 chuẩn bị được gửi đi: Dạng khung dữ liệu. 42](#_bookmark55)

[Hình 31. Gói tin ở Router1 Hà Nội. 42](#_bookmark56)

[Hình 32. Gói tin ở Cloud0. 43](#_bookmark57)

[Hình 33. Gói tin ở Router2 TP. Hồ Chí Minh. 43](#_bookmark58)

[Hình 34. Gói tin phản hồi của PC2 về PC0: Mô hình OSI. 44](#_bookmark59)

[Hình 35. Gói tin phản hồi của PC2 về PC0: Dạng khung dữ liệu. 44](#_bookmark60)

MỤC LỤC

## [PHẦN MỘT: TỔNG QUAN VỀ MẠNG ETHERNET, WIRELESS LAN VÀ](#_bookmark0) [FRAME RELAY 6](#_bookmark0)

1. [**Mạng Ethernet 6**](#_bookmark1)
   1. [Khái niệm về Ethernet 6](#_bookmark2)
   2. [Lịch sử hình thành và phát triển 6](#_bookmark3)
   3. [Các thành phần mạng Ethernet 8](#_bookmark4)
   4. [Các chuẩn và tốc độ của Ethernet 9](#_bookmark6)
   5. [Ethernet ở lớp Liên kết dữ liệu (Data link) 11](#_bookmark8)
   6. [Hoạt động của Ethernet 14](#_bookmark13)

## [Mạng Wireless LAN 15](#_bookmark14)

* 1. [Khái niệm về Wireless LAN 15](#_bookmark15)
  2. [Lịch sử hình thành và phát triển 16](#_bookmark17)
  3. [3 mô hình mạng WLAN phổ biến 17](#_bookmark19)
  4. [Ưu điểm và nhược điểm của mạng WLAN 18](#_bookmark20)
  5. [Hệ thống hạ tầng cần thiết cho mạng WLAN 20](#_bookmark23)
  6. [Các chế độ mạng không dây thường gặp 22](#_bookmark26)
  7. [Chuẩn công nghệ Wifi 24](#_bookmark30)
  8. [Cách bảo mật mạng WLAN không dây 28](#_bookmark31)

## [Frame Relay 30](#_bookmark32)

* 1. [Khái niệm 30](#_bookmark33)
  2. [Cấu trúc khung của Frame relay 31](#_bookmark34)
  3. [Cách thức hoạt động 32](#_bookmark37)
  4. [Ưu điểm và nhược điểm của Frame relay 33](#_bookmark38)

[PHẦN HAI: MÔ PHỎNG MẠNG ETHERNET, WIRELESS LAN VÀ FRAME](#_bookmark39) [RELAY 34](#_bookmark39)

1. [Mô phỏng mạng Ethernet 34](#_bookmark40)
2. [Mô phỏng Wireless 37](#_bookmark47)
3. [Mô phỏng Frame Relay 40](#_bookmark52)

# PHẦN MỘT: TỔNG QUAN VỀ MẠNG ETHERNET, WIRELESS LAN VÀ FRAME RELAY

## Mạng Ethernet

* 1. **Khái niệm về Ethernet**

Ethernet là một họ lớn và đa dạng các công nghệ mạng máy tính thường dùng trong các mạng local area network (LAN). Tên gọi Ethernet xuất phát từ khái niệm Ete trong ngành vật lý học. Nó được giới thiệu thương mại vào năm 1980 và lần đầu tiên được tiêu chuẩn hoá vào năm 1983 thành IEEE 802.3, kể từ đó nó được chỉnh sửa để hỗ trợ bit rate cao hơn và khoảng cách kết nối xa hơn. Theo thời gian, Ethernet đã thay thế hoàn toàn các công nghệ LAN nối dây như token ring, FDDI và ARCNET.

10BASE5 Ethernet nguyên thủy dùng cáp đồng trục (coaxial cable) làm shared medium (phương tiện/môi trường được chia sẻ), trong khi các phiên bản Ethernet mới hơn dùng cáp xoắn đôi (twisted pair) và các liên kết sợi quang học trong việc kết nối với các hub hoặc switch. Theo quá trình phát triển, tốc độ truyền dữ liệu Ethernet đã tăng từ 2.94Mbit/s ban đầu lên đến tốc độ gần đây nhất là 100Gbit/s. Các tiêu chuẩn Ethernet gồm nhiều phiên bản phát tín hiệu và nối dây của tầng vật lý của mô hình OSI khi sử dụng Ethernet.

Các hệ thống giao tiếp qua Ethernet chia một dòng dữ liệu (data stream) thành các mảnh ngắn hơn gọi là các frame. Mỗi frame gồm có địa chỉ nguồn, địa chỉ đích, và dữ liệu kiểm tra lỗi sao cho các frame bị hư hại có thể được phát hiện và loại bỏ; thường gặp nhất là các protocol tầng cao hơn kích hoạt (trigger) việc truyền lại các frame bị mất. Đối với mô hình OSI, Ethernet cung cấp các dịch vụ lên đến và bao gồm tầng liên kết dữ liệu.

## Lịch sử hình thành và phát triển

Ethernet được phát triển tại Xerox PARC từ năm 1973 đến năm 1974. Nó được lấy cảm hứng từ ALOHAnet, một phần nghiên cứu trong luận án tiến sĩ của Robert Metcalfe. Metcalfe lần đầu ghi lại ý tưởng này trong một mẩu giấy ghi nhớ vào ngày 22 tháng 5 năm 1973, trong đó ông đặt tên công nghệ theo Luminiferous aether (ê-te) với ý nghĩa là một "phương tiện thụ động hoàn toàn có ở khắp nơi để lan truyền sóng điện từ". Vào năm 1975,

Xerox đã nộp đơn xin cấp bằng sáng chế trong đó Metcalfe, David Boggs, Chuck Thacker, và Butler Lampson là những người phát minh. Vào năm 1976, sau khi hệ thống đã được vận hành ở PARC, Metcalfe và Boggs đã xuất bản một bài báo quan trọng.

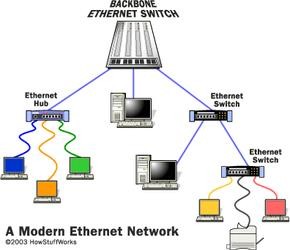
Metcalfe đã rời Xerox vào tháng 6 năm 1979 để lập công ty 3Com. Ông đã thuyết phục Digital Equipment Corporation (DEC), Intel, và Xerox hợp tác để quảng bá tiêu chuẩn Ethernet. Tiêu chuẩn được gọi là "DIX", viết tắt của "Digital/Intel/Xerox", cụ thể là Ethernet 10 Mbit/s, với các địa chỉ nguồn và đích 48-bit và một trường toàn cục 16 bit kiểu Ethertype. Tiêu chuẩn được công bố vào ngày 30 tháng 9 năm 1980 với tiêu đề "The Ethernet, A Local Area Network. Data Link Layer and Physical Layer Specifications". Version 2 được xuất bản vào tháng 11 năm 1982 đã định nghĩa Ethernet II hiện nay. Các nỗ lực tiêu chuẩn hóa chính thức được tiến hành cùng thời gian và đã dẫn đến việc xuất bản IEEE 802.3 vào ngày 23 tháng 6 năm 1983.

Ethernet khởi đầu cạnh tranh với hai hệ thống lớn có bản quyền là Token Ring và Token Bus. Vì Ethernet đáp ứng được thực tiễn thị trường và tiến đến việc nối dây cáp xoắn đôi giá rẻ và phổ biến khắp mọi nơi, các protocol có bản quyền này nhanh chóng bị tụt hậu và cho đến cuối thập năm 1980, Ethernet trở thành công nghệ mạng có ưu thế hoàn toàn trên thị trường. Và công ty 3Com cũng trở thành người chơi chính. 3Com đã bán các sản phẩm đầu tiên của họ là Network Interface Controller (NIC) 3C100 hỗ trợ Ethernet 10 Mbit/s vào tháng 3 năm 1981, cũng năm đó họ đã bắt đầu bán các adapter cho PDP-11 và VAX, cũng như các máy tính Intel và Sun Microsystems trên nền tảng Multibus. Unibus của DEC nhanh chóng bước theo adapter Ethernet, DEC đã bán và sử dụng chúng trong nội bộ công ty để dựng nên mạng tập đoàn (corporate network) của chính họ với hơn 10,000 nốt vào năm 1986, trở thành một trong những mạng máy tính lớn nhất thế giới tại thời điểm đó. Một card adapter Ethernet dành cho IBM PC đã được phát hành vào năm 1982, và tới năm 1985, 3Com đã bán được 100,000 cái. Adapter Ethernet dựa trên cổng song song đã từng được chế tạo và có cả driver cho các hệ điều hành DOS và Windows. Tới đầu thập niên 1990, Ethernet đã trở nên thịnh hành, được xem là một đặc tính bắt buộc phải có ở những máy tính hiện đại, và các cổng Ethernet đã bắt đầu xuất hiện trên một vài PC và trên phần lớn workstation (máy trạm). Quá trình này được thúc đẩy nhanh hơn nữa với sự ra

đời của 10BASE-T và modular connector nhỏ của nó, trong đó các cổng Ethernet đã xuất hiện thậm chí ở cả các bo mạch chủ cấp thấp (low-end motherboard).

Từ đó, công nghệ Ethernet dần phát triển để đáp ứng các yêu cầu về thị trường và bandwidth mới. Ngày nay, ngoài máy tính, Ethernet còn được sử dụng để liên kết các appliance (công cụ, dụng cụ) và các thiết bị di động cá nhân. Ethernet được sử dụng trong các ứng dụng công nghiệp và đang nhanh chóng thay thế các hệ thống truyền dữ liệu hiện có trong các mạng viễn thông trên thế giới.

## Các thành phần mạng Ethernet

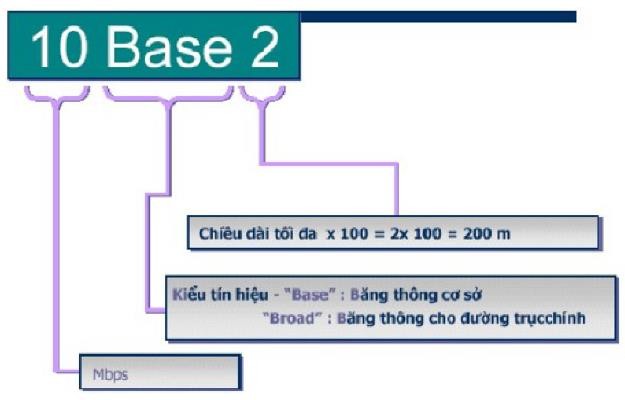


*Hình 1. Các thành phần mạng Ethernet.*

Các thành phần chính trong mạng Ethernet:

* + - Data Terminal Equiqment (DTE): là các thiết bị truyền và nhận dữ liệu. DTEs thường là PC, File Server, Print Server,…
    - Data Communication Equiqment (DCE): là các thiết bị kết nối mạng cho phép nhận và chuyển khung trên mạng. DCEs có thể là các thiết bị độc lập như Repeater, Switch, Router hoặc các khối giao tiếp thông tin như Card mạng, Moderm,…
    - Interconnecting Media: có thể sử dụng nhiều loại cáp như cáp xoắn đôi, cáp đồng trục mỏng, cáp đồng trục dày, cáp sợi quang,…Cáp xoắn đôi có thể chia thành nhiều kiểu, phổ biến hiện nay là:
* **CAT5E** là loại cáp có thể truyền tải dữ liệu vô cùng tối ưu lên đến 1000 Mbps (1Gbps), điều này giúp quá trình sử dụng của bạn trở nên thoải mái hơn. Ngoài ra, nó còn có đặc tính ưu việt là ít nhiễm chéo giúp quá trình mượt mà và luôn ổn định.
* **CAT6** có phần tương tự với loại cáp CAT5E đều mang đến người dùng trải nghiệm ổn định. Tuy nhiên, CAT6 lại có băng thông gấp 2,5 lần so với CAT5E (cụ thể là 250 MHz) và tốc độ cũng có thể đạt 10 000Mbps (10Gbps) với khoảng cách dưới 100m.
* **CAT6A** có đặc tính tránh nhiễu sóng hiệu quả nhờ có thêm lớp bảo vệ. Bên cạnh đó, nó còn có đặc điểm nổi bật là băng thông đạt mức 500 MHz gấp đôi so với CAT6 và tốc độ truyền lên đến 10 000Mbps (10Gbps).

## Các chuẩn và tốc độ của Ethernet



*Hình 2. Cách đọc tên các chuẩn Ethernet.*

* + 1. *Hệ thống Ethernet tiêu chuẩn (10Mbps)*

**10Base5:** Đây là chuẩn Ethernet đầu tiên, sử dụng cáp đồng trục loại dày. Tốc độ đạt được 10Mbps, sử dụng băng tần cơ sở, chiều dài cáp tối đa cho một phân đoạn là 500m. **10Base2:** Còn có tên gọi là “thin Ethernet”. Chuẩn này dựa trên hệ thống cáp đồng

trục mỏng với tốc độ 10Mbps, chiều dài tối đa của mỗi phân đoạn là 200m.

**10BaseT:** Chữ T là viết tắt của twisted (cáp xoắn cặp). Chuẩn này hoạt động với tốc độ 10Mbps và dựa trên hệ thống cáp xoắn cặp Cat3 trở lên.

**10BaseF:** Ra đời năm 1993, đây là chuẩn Ethernet dùng sợi quang hoạt động ở tốc độ 10Mbps, chữ F là viết tắt của Fiber optic (sợi quang).

* + 1. *Hệ thống Fast Ethernet (100Mbps)*

**100BaseT:** Chuẩn Ethernet hoạt động ở tốc độ 100Mbps trên cả cáp xoắn cặp lẫn cáp sợi quang.

* **100BASE-TX**: Được sử dụng cho giao tiếp điểm-điểm song công với hai cặp cáp xoắn. Một cặp nhận tín hiệu trong khi cặp kia gửi chúng. 100BASE-TX sử dụng cáp RJ- 45 để kết nối vật lý và hỗ trợ độ dài phân đoạn lên đến 100 mét.
* **100BASE-T4**: Một trong những phiên bản Fast Ethernet sớm nhất. Nó sử dụng cáp xoắn đôi CAT-3 và yêu cầu bốn cặp cáp để giao tiếp.
* **100BASE-FX**: Chuẩn cáp quang này sử dụng bước sóng ánh sáng hồng ngoại mỏng để liên lạc qua hai sợi cáp. Hai sợi được sử dụng để truyền và nhận tín hiệu; một cái gửi và cái kia nhận để có thể giao tiếp song công.
  + 1. *Hệ thống Gigabit Ethernet (1Gbps)*

**1000BaseX** gồm 3 loại:

* **1000Base-SX:** sử dụng sợi quang với bước sóng ngắn. Tiêu chuẩn này rất phổ biến cho các liên kết nội bộ trong các tòa nhà văn phòng lớn, các cơ sở đồng địa điểm và trao đổi Internet trung lập với nhà mạng.
* **1000Base-LX:** sử dụng sợi quang với bước sóng dài. Khoảng cách truyền lớn đạt 5km với single mode và 550m với multimode.
* **1000Base-CX:** chuẩn đầu tiên của kết nối Gigabit Ethernet với khoảng cách tối đa là 25 mét sử dụng cáp xoắn đôi.

**1000BaseT:** hoạt động ở tốc độ 1Gbps, băng tần cơ sở, trên cáp xoắn cặp Cat5 trở

lên.

* + 1. *Hệ thống Ten-gigabit Ethernet (10Gbps***)** *Đối với cáp sợi quang:*

**10GBase-SR:** sử dụng sợi quang multi-mode với bước sóng 850nm

**10GBase-LR:** sử dụng sợi quang single-mode với bước sóng 1310nm

**10GBase-ER:** sử dụng sợi quang single-mode với bước sóng 1550nm

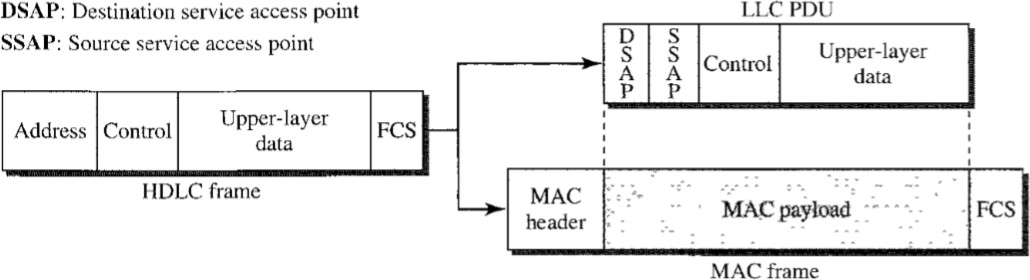
Khoảng cách truyền của các chuẩn trên có thể phụ thuộc vào loại cáp đang sử dụng.

*Đối với cáp xoắn đôi:*

**10GBase-T:** là tiêu chuẩn được phát hành vào năm 2006 để cung cấp kết nối 10 Gbit/s qua cáp xoắn đôi không hoặc có vỏ bọc, với khoảng cách lên đến 100 mét, CAT6A được yêu cầu để đạt được khoảng cách đầy đủ và CAT6 có thể đạt tới 55 mét.

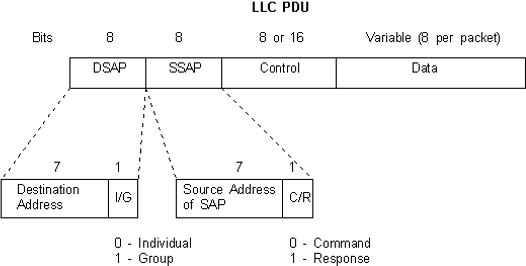
## Ethernet ở lớp Liên kết dữ liệu (Data link)

IEEE đã chia lớp liên kết dữ liệu thành hai lớp con: Logical Link Control (LLC) và Media Access Control (MAC). LLC cung cấp một giao thức điều khiển liên kết dữ liệu duy nhất cho tất cả các mạng IEEE LAN. Theo cách này, LLC khác với lớp con MAC - cung cấp các giao thức khác nhau cho các mạng LAN khác nhau. Lớp con MAC chi phối hoạt động của các phương thức truy cập, đống khung dữ liệu từ lớp trên. Một khung trong HDLC có thể được chia thành PDU ở LLC và khung ở MAC.



Tầng con LLC chủ yếu quan tâm đến:

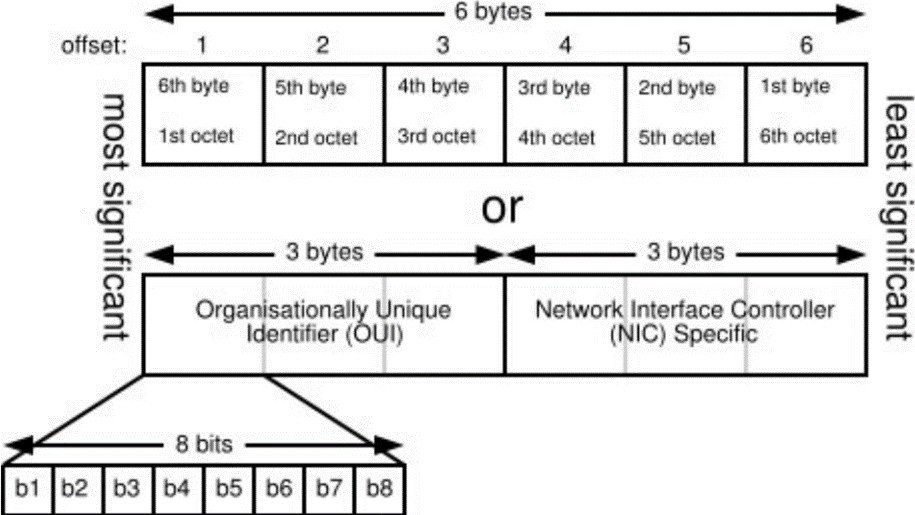
* + - Ghép kênh (multiplexing) các giao thức được truyền qua tầng MAC (khi truyền) và phân kênh (demultiplexing) chúng (khi nhận).
    - Theo yêu cầu, cung cấp chức năng điều khiển lỗi và luồng.
    - Giao thức cho LLC được đặc tả trong chuẩn IEEE 802.2



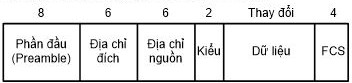
LLC định nghĩa một Protocol Data Unit có phần giống với HDLC. Header chứa trường điều khiển; trường này được sử dụng để kiểm soát luồng và lỗi. Hai trường khác xác định giao thức lớp trên tại nguồn và đích sử dụng LLC.

Địa chỉ MAC:

Bao gồm 2 phần OUI và NIC. OUI (được gọi là ký hiệu nhận dạng duy nhất theo tổ chức) sẽ chỉ ra nhà sản xuất ra NIC, còn 3 bytes sau sẽ là đặc trưng cho từng NIC. Vì vậy trên thế giới mỗi NIC sẽ có 1 địa chỉ MAC riêng biệt.



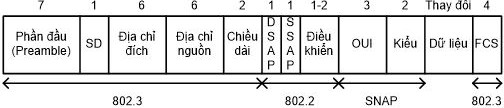
Đặc tả Ethernet ban đầu được sở hữu bởi bộ ba công ty Digital, Intel và Xerox đặt tên là Ethernet II(DIX) vào năm 1978. Năm 1980, tổ chức IEEE khởi động dự án 802, sau đó vào năm 1983, khung Ethernet theo chuẩn IEEE 802.3 được sử dụng. IEEE nhận ra rằng trường 1 byte DSAP trong header của LLC là quá nhỏ, kết quả là IEEE giới thiệu ra một định dạng khung tin mới gọi là giao thức truy cập mạng con SNAP.



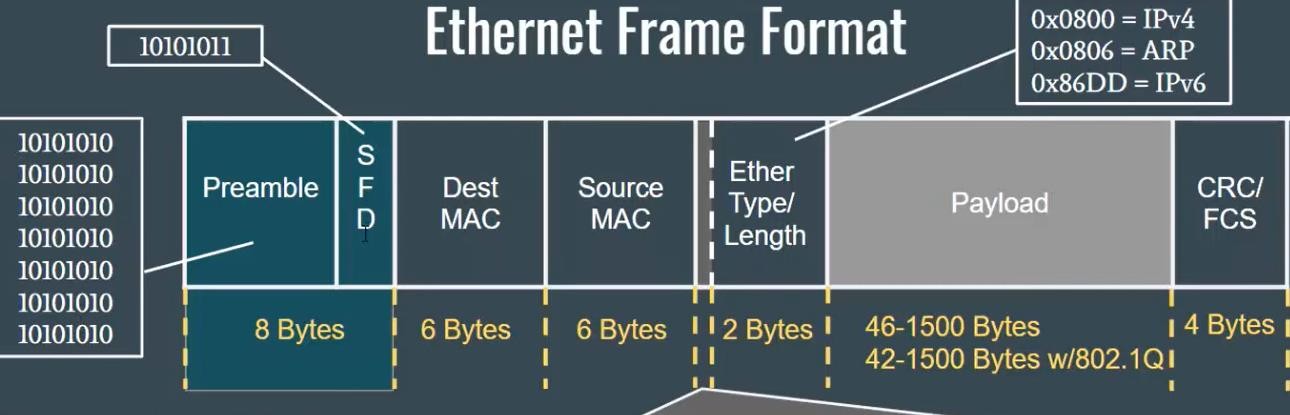
*Hình 3. Ethernet II frame*



*Hình 4. IEEE 802.3 frame.*



*Hình 5. IEEE 802.3 frame có thêm SNAP*



*Hình 6. Cấu trúc khung của ethernet*

Cấu trúc khung của Ethernet bao gồm:

* + - Preamble và SD (802.3): Cho phép đồng bộ các khung tin, xác định điểm bắt đầu của khung. Đây chỉ là phần được thêm vào không tính là một phần của khung.
    - Địa chỉ MAC đích đến
    - Địa chỉ MAC nguồn
    - Kiểu (DIX/Egternet II): Chỉ ra loại dữ liệu đang mang bên trong phần dữ liệu.
    - Chiều dài(IEEE 802.3): Chỉ ra chiều dài của dữ liệu bên trong một khung tin.
    - Payload hay Data and Padding: chứa Data của các lớp trên và các bit được thêm vào
    - CRC/FCS: Kiểm tra và phát hiện lỗi.

Mỗi header của khung tin Ethernet đều có các trường để chỉ ra loại dữ liệu đang mang bên trong trường dữ liệu của khung tin. Trường kiểu giao thức (protocol type) cho phép máy nhận biết cách làm thế nào để diễn dịch được các dữ liệu bên trong khung tin nhận được. Ví dụ, một router cần biết khi nào thì khung tin chứa một gói tin IP, IPX….

DIX dùng trường kiểu giao thức. Phiên bản do IEEE định nghĩa ban đầu thì dùng 2 byte này như là trường chiều dài. Vì vậy, để phân biệt, nếu trường này có giá trị nhỏ hơn 1500 thì khung thuộc IEEE 802.3, nếu có giá trị lớn hơn 1536 thì khung sẽ là chuẩn Ethernet II. Đối với IEEE 802.3, để nhận biết kiểu dữ liệu sẽ dựa vào LLC PDU.

## Hoạt động của Ethernet

Mỗi máy Ethernet, hay còn gọi là máy trạm, hoạt động độc lập với tất cả các trạm khác trên mạng và khôgn có một trạm điều khiển trung tâm. Thông qua một đường truyền tín hiệu gọi là đường trung gian thì các trạm đều kết nối với Ethernet. Tín hiệu Ethernet được gửi theo chuỗi, từng bit, qua đường trung gian tới tất cả các trạm khác nhau.

Lớp liên kết dữ liệu được chia thành hai phần: Logical Link Control (LLC) và Media Access Control (MAC).

Điều khiển liên kết logic thiết lập đường dẫn cho dữ liệu trên Ethernet để truyền giữa các thiết bị . Kiểm soát truy cập phương tiện sử dụng địa chỉ phần cứng được chỉ định cho Network Interface Cards (NIC) để xác định một máy tính hoặc thiết bị để hiển thị nguồn và đích truyền dữ liệu.

Ethernet truyền các gói dữ liệu trong lớp liên kết dữ liệu này bằng cách sử dụng một thuật toán được gọi là CSMA/CD (Carrier Sense Multiple Access with Collision Detection ). CSMA/CD được sử dụng làm tiêu chuẩn cho Ethernet để giảm xung đột dữ

liệu và tăng truyền dữ liệu thành công. Thuật toán kiểm tra đầu tiên để xem nếu có lưu lượng truy cập trên mạng. Nếu nó không tìm thấy bất kỳ, nó sẽ gửi đi phần thông tin đầu tiên để xem có xảy ra va chạm hay không.

Nếu bit đầu tiên này thành công, sau đó nó sẽ gửi các bit khác trong khi vẫn thử nghiệm các va chạm. Nếu xảy ra va chạm, thuật toán tính toán thời gian chờ đợi và sau đó bắt đầu xử lý lại tất cả cho đến khi quá trình truyền hoàn tất.

## Mạng Wireless LAN

* 1. **Khái niệm về Wireless LAN**

Wireless LAN (WLAN) là một kỹ thuật phân phối mạng không dây, hỗ trợ nhiều thiết bị cùng lúc kết nối với mạng internet, thực hiện thông qua giao thức chuẩn. Có thể hiểu đơn giản WLAN hay wireless local area network chính là mạng cục bộ không dây.



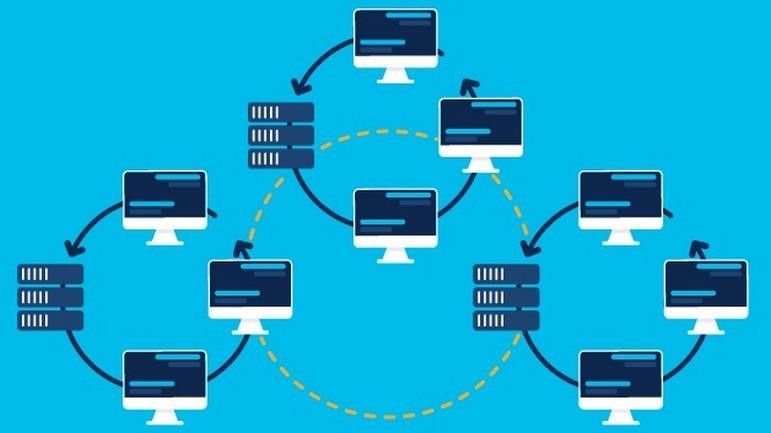
*Hình 7. Các thiết bị kết nối mạng WLAN.*

Có nghĩa là thay vì liên kết hệ thống mạng qua dây cáp truyền thống, WLAN lại ứng dụng tín hiệu radio, hồng ngoại để hỗ trợ thiết bị có thể liên lạc với nhau. Cách thức liên kết này loại bỏ sự cồng kềnh của hệ thống dây cáp, tiết kiệm chi phí đầu tư phần cứng.

Mặc dù kết nối theo kiểu không dây nhưng WLAN vẫn đảm bảo tín hiệu đường truyền, tương tác giữa các thiết bị. Chỉ cần vẫn còn đang trong phạm vi phủ sóng, thiết bị của bạn vẫn có thể truy cập internet một cách dễ dàng.

## Lịch sử hình thành và phát triển

Kỹ thuật liên kết mạng không dây chính thức ra đời từ năm 1990. Đây được xem từng bước đột phá giúp mạng internet toàn cầu ngày càng phổ cập rộng rãi. Để có thể hoàn thiện như ngày nay, WLAN phải trải qua nhiều giai đoạn từ khâu nghiên cứu, bổ sung tinh chỉnh và ứng dụng vào đời sống.



*Hình 8. Mô hình liên kết mạng WLAN.*

**Giai đoạn năm 1990:** Lần đầu tiên, kỹ thuật kết nối mạng không dây ra mắt người dùng toàn cầu. Khi đó các thiết bị được hỗ trợ hoạt động tại băng tần 900Mhz, tốc độ truyền dữ liệu đạt 1Mbps. Con số này khá thấp so với tốc độ 10Mbps của hệ thống mạng có dây thời điểm bấy giờ.

**Giai đoạn từ năm 1992 đến 1996:** Băng tần của WLAN dần nâng lên 2.4Ghz. Tuy nhiên tần số lại chưa có sự thống nhất cao.

**Giai đoạn năm 1997 đến 1999:** IEEE chính thức thông qua hai chuẩn 802.11a và 802.11b. Cụ thể, 802.11b sở hữu tốc độ đường truyền 11Mbps. Các thiết bị thiết kế theo chuẩn 802.11b dần trở nên phổ biến.

**Giai đoạn năm 2003:** IEEE cấp phép thêm chuẩn 802.11g có khả năng tiếp nhận đường chuyền từ cả hai đầu dây dẫn với băng tần 2.4Ghz và 5Ghz. Tốc độ đường truyền đã lên tới 54Mbps.

## 3 mô hình mạng WLAN phổ biến

Hiện nay, mạng WLAN chia thành 3 mô hình hoạt động chủ yếu. Bao gồm mô hình cơ sở, mô hình độc lập và mô hình mở rộng.

## Mô hình độc lập IBSS (Independent Basic Service Set)

Trong mô hình WLAN độc lập, thường bao gồm các máy tính kết nối mạng quy tụ tại không gian nhỏ để hình thành nên kết nối ngang cấp (peer-to-peer) giữa chúng. Từ đó tạo thành kết nối nhanh cấp. Toàn bộ nút kết nối di động đều có khả năng trao đổi thông tin trực tiếp, không phụ thuộc vào quản trị mạng. Mô hình mạng nhỏ nhất trong chuẩn

802.11 là 2 máy client liên lạc trực tiếp với nhau. Mô hình mạng này có nhược điểm lớn về vùng phủ sóng bị giới hạn, mọi client đều phải liên lạc được lẫn nhau.

## Mô hình cơ sở BSS (Basic Service Sets)

Mô hình mạng cơ sở là một topology nền tảng của mạng 802.11. Tại mô hình WLAN cơ sở tập trung nhiều điểm kết nối Access Point liên kết chặt chẽ với hệ thống đường trục hữu tuyến. Đây là mô hình mạng cho phép thiết bị di động hoạt động ổn định trong phạm vi phủ sóng thuộc một cell.

Trong đó, Access Point sẽ làm nhiệm vụ điều khiển cell, đồng thời điều chỉnh lưu lượng đến mạng. Access point phục vụ như một điểm truy cập duy nhất cho mọi thiết bị muốn sử dụng BSS. Nó quảng cáo sự tồn tại của BSS để các thiết bị tìm thấy và kết nối với nó. Ngoài ra access point quảng cáo mạng không dây bằng SSID (Service Set Identifier). SSID xác định dịch vụ không dây, còn để client nhận diện acces point thì access point dùng một mã định danh (BSSID) dựa trên địa chỉ MAC của nó. Để tham gia BSS thì client phải gửi yêu cầu cho access point và chờ được chấp nhận. Khi được chấp nhận thì thiết bị sẽ trở

thành client 802.11 (STA) của BSS. Như vậy, các thiết bị thường không trực tiếp tương tác với nhau mà tương tác với Access Point.

## Mô hình mở rộng ESS (Extended Service Set)

Bình thường một Access Point không thể phủ sóng toàn bộ khu vực rộng lớn. Mô hình mở rộng gồm tập hợp nhiều BSSs, nơi cho phép Access Point tương tác với nhau nhằm luân chuyển lưu lượng giữa các BSS. Các access point phải được kết nói với nhau chung một hạ tầng. Các client ở vị trí nào đều có chung một SSID nhưng khác BSSID để phân biệt acces point với nhau. Từ đó đảm bảo quá trình luân chuyển giữa các BSS luôn được ổn định. Mặt khác, BSS còn thực hiện chức năng kết nối thiết bị di động, tương tác với những BSS khác.

## Ưu điểm và nhược điểm của mạng WLAN Ưu điểm



*Hình 9. Hệ thống WLAN cho phép thiết bị kết nối mạng nhanh chóng.*

Ưu điểm của mạng WLAN nằm ở tính tiện lợi, di động cao, triển khai đơn giản, có khả năng mở rộng linh hoạt.

* **Tiện lợi:** Hệ thống mạng WLAN cho phép thiết bị kết nối mạng nhanh chóng, số lượng thiết bị kết nối cùng lúc lớn hơn so với mạng có dây.
* **Tính di động cao:** Sự bùng nổ của mạng không dây giúp phổ cập rộng rãi mạng internet. Người dùng có thể truy cập mạng internet tại nhiều nơi.
* **Dễ dàng triển khai:** Trong mô hình mạng không dây, người ta chỉ yêu cầu một điểm truy cập, không cần đến nhiều dây nối phức tạp. Cách thức triển khai mạng WLAN nhìn chung đơn giản hơn so với mạng có dây.
* **Khả năng mở rộng linh hoạt:** Mạng WLAN có thể dễ dàng mở rộng, cho phép tăng thiết bị truy cập thông qua quá trình lắp đặt thêm cáp.

## Nhược điểm



*Hình 10. Mạng WLAN tồn tại nhược điểm về tính bảo mật.*

Song song với nhiều ưu điểm, mạng WLAN cũng vẫn còn một số hạn chế nhất định về mặt bảo mật, phạm vi truy cập, tốc độ và độ tin cậy.

* **Hạn chế về mặt bảo mật:** Tùy rằng tạo điều kiện để người dùng kết nối dễ dàng nhưng WLAN lại dễ bị hack. Tình trạng người dùng bị thu thập thông tin trái phép vẫn thường xuyên xảy ra.
* **Phạm vi truy cập còn hạn chế:** Thông thường mạng WLAN chỉ phủ sóng truy cập trong một phạm vi nhất định. Trường hợp muốn mở rộng phạm vi, bạn phải bổ sung repeater hoặc Access Point.
* **Độ tin cậy chưa cao:** WLAN sử dụng sóng vô tuyến thay vì hệ thống dây cáp. Chính vì vậy tín hiệu chưa thực sự ổn định cho lắm.
* **Tốc độ mạng còn chậm:** Tốc độ đường truyền mạng trong chưa cao bằng hệ thống mạng có dây. Càng nhiều người dùng truy cập, tốc mạng lại càng chậm.

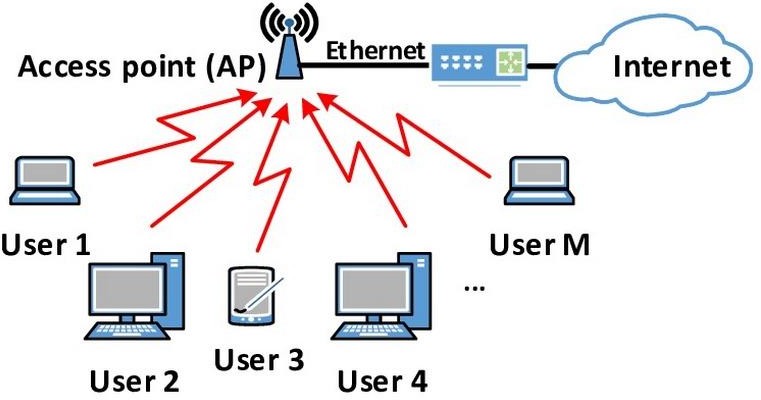
## Hệ thống hạ tầng cần thiết cho mạng WLAN

Để một hệ thống mạng WLAN hoạt động đòi hỏi phải có đầy đủ hạ tầng cần thiết.

Chẳng hạn như điểm truy cập, thiết bị máy khách.

* + 1. *Điểm truy cập*

Điểm truy cập AP (Access Point) giữ nhiệm vụ cấp phép để máy khách có thể truy cập vào mạng WLAN. Mỗi điểm truy cập lại ứng với một thiết bị Full Duplex, tốc độ tương đương với Ethernet.



*Hình 11. Mô hình Access Point.*

Mỗi Access Point có thể hoạt động theo một trong ba chế độ chính. Cụ thể là chế độ Root Mode, Bridge Mode và Repeater Mode.

* + 1. *Thiết bị máy khách*



*Hình 12. Card PCI Wireless.*

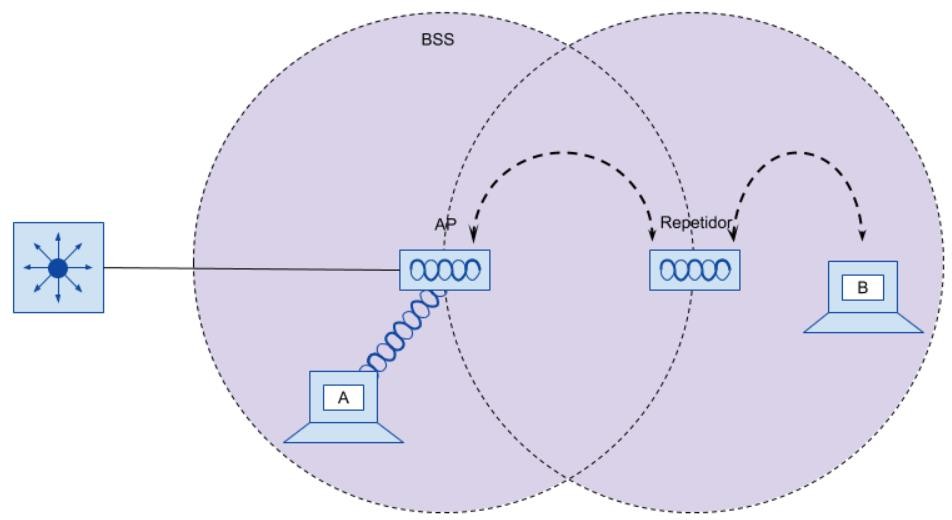
Thiết bị máy khách trong WLAN thường bao gồm 3 chủng loại thiết bị chính. Trong đó, mỗi thiết bị lại thực hiện một vai trò riêng.

* **Card PCI Wireless:** Giữ nhiệm vụ kết nối máy khách với mạng không dây WLAN.
* **Card PCMCIA Wireless:** Sử dụng phổ biến trong laptop và nhiều loại thiết bị cá nhân khác.
* **Card USB Wireless:** Thiết kế vô cùng nhỏ gọn, tháo lắp đơn giản, dễ dàng cắm ngay cả khi thiết bị vẫn hoạt động.

## Các chế độ mạng không dây thường gặp

* + 1. *Repeater*

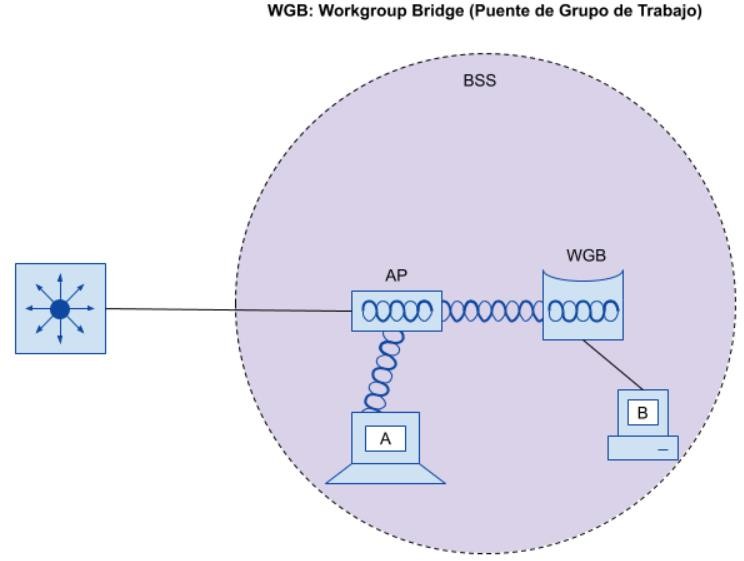
Để mở rộng vùng phủ sóng không dây, ta có thể dùng dây cáp đấu nối đến một repeater mới để bổ sung. Trong một số trường hợp không thể đấu nối dây ta thường cấu hình access point ở chế độ repeater nhận tín hiệu từ một access point phát. Mục đích là để mở rộng vùng phủ sóng mà không cần kết nối dây.



*Hình 13. Mô hình mạng Repeater.*

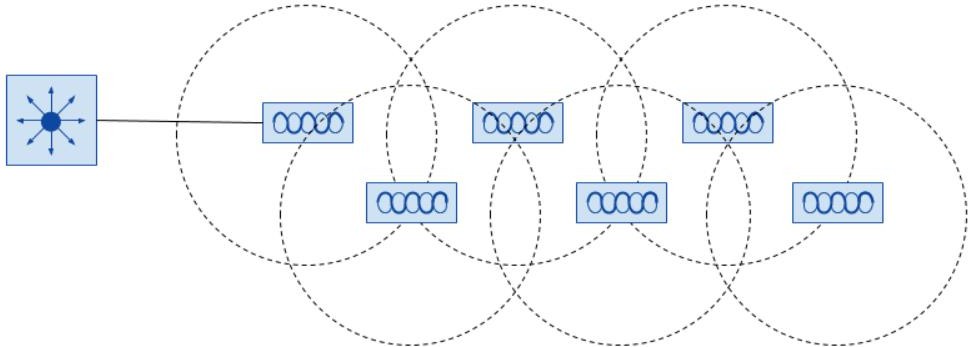
* + 1. *Workgroup bridge*

Đối với các thiết bị không có khả năng kết nối không dây như PC chỉ có card mạng mà không có card wifi, nhưng vẫn muốn kết nối với một access point ta có thể sử dụng workgroup bridge để kết nối không dây.



*Hình 14. Mô hình mạng Workgroup bridge.*

* + 1. *Mesh network*

Mô hình mesh cơ bản giống như mô hình repeater. Cả hai đều dùng mạng không dây để kết nối giữa các thiết bị. Điểm khác biệt chính là SSID ở mô hình mesh được đồng bộ, chúng ta chỉ cần cấu hình một thiết bị. khi đi đến những vùng của access point khác nhau ta sẽ không phải kết nối lại.

*Hình 15. Mô hình mạng Mesh.*

## Chuẩn công nghệ Wifi

*2.7.1. IEEE 802.11*

Là chuẩn đầu tiên mô tả hoạt động của WLAN. Chuẩn này bao gồm các công nghệ truyền dẫn có sẵn như DSSS (Direct Sequence Spread Spectrum), FHSS (Frequency Hopping Spread Spectrum) và hồng ngoại.

802.11 chỉ hoạt động ở các tốc độ 1Mbps và 2Mbps. Nếu hệ thống hoạt động ở một tốc độ nào khác ngoài 1Mbps và 2Mbps thì không thể giao tiếp với các thiết bị tương thích

802.11 khác. Với lý do đó, các sản phẩm không dây thiết kế theo chuẩn 802.11 ban đầu dần không được sản xuất nữa.

* + 1. *IEEE 802.11b (Wifi 1)*

Từ tháng 6 năm 1999, IEEE mở rộng chuẩn 802.11 ban đầu và tạo ra các đặc tả kỹ thuật cho 802.11b. Chuẩn 802.11b hỗ trợ băng thông 11Mbps, ngang với tốc độ Ethernet thời bấy giờ. Đây là chuẩn WLAN lần đầu tiên được chấp nhận trên thị trường, sử dụng tần số 2,4 GHz. Chuẩn 802.11b sử dụng kỹ thuật điều chế khoá mã bù (Compementary Code Keying – CCK) và dùng kỹ thuật trải phổ trực tiếp giống như chuẩn 802.11 nguyên bản. Chuẩn này không mô tả hệ thống FHSS.

Các thiết bị tương thích 802.11b thì mặc định sẽ tương thích 802.11. Chuẩn chỉ hoạt động ở băng tần 2,4GHz giữa 2,4000GHz và 2,4835GHz.

* Ưu điểm: Giá thành thấp nhất, tầm phủ sóng tốt và không dễ bị che khuất.
* Nhược điểm: Tốc độ tối đa thấp, có thể bị nhiễu bởi các thiết bị gia dụng.
  + 1. *IEEE 802.11a (Wifi 2)*

IEEE đưa ra chuẩn mở rộng thứ hai cũng dựa vào 802.11 đầu tiên đó là 802.11a. Chuẩn 802.11a sử dụng tần số 5GHz, tốc độ 54Mbps. Chuẩn 802.11a cũng sử dụng kỹ thuật trải phổ khác với chuẩn 802.11b, đó là kỹ thuật trải phổ theo phương pháp đa phân chia tần số trực giao (Orthogonal Frequency Division Multiplexing-OFDM). Đây được coi là kỹ thuật trội hơn so với trải phổ trực tiếp (DSSS). Do chi phí cao hơn, 802.11a thường chỉ được dùng trong các mạng doanh nghiệp, ngược lại, 802.11b thích hợp hơn cho nhu cầu gia đình.

Tuy nhiên, do tần số cao hơn tần số của chuẩn 802.11b nên tín hiệu của 802.11a gặp nhiều khó khăn hơn khi xuyên tường các vật chất cản khác. Vùng phủ sóng từ 30-70 m. Do 802.11a và 802.11b sử dụng tần số khác nhau, hai công nghệ này không tương thích với nhau. Một vài hãng sản xuất bắt đầu cho ra đời sản phẩm “lai” 802.11a/b, nhưng các sản phẩm đơn thuần này chỉ đơn thuần là cung cấp 2 chuẩn sóng Wi-Fi cùng lúc.

* Ưu điểm: Tốc độ cao, với tần số 5GHz tránh được sự xuyên nhiễu từ các thiết bị khác.
* Nhược điểm: Giá thành đắt, tầm phủ sóng ngắn hơn và dễ bị che khuất, hoạt động trên tần số 5GHz, tốc độ truyền tải lên đến 54Mbps nhưng không xuyên qua được vật cản. Hiện nay dạng chuẩn này rất ít được sử dụng.
  + 1. *IEEE 802.11g (Wifi 3)*

Năm 2002 và 2003, các sản phẩm WLAN hỗ trợ chuẩn mới hơn được gọi là 802.11g, được đánh giá cao trên thị trường, chuẩn này cố gắng kết hợp tốt nhất 802.11a và 802.11b. Chuẩn 802.11g hỗ trợ băng thông 54Mbps và sử dụng tần số 2,4GHz cho phạm vi phủ sóng lớn hơn. 802.11b, nghĩa là các điểm truy cập (access point – AP) 802.11g sẽ làm việc với card mạng Wi-Fi chuẩn 802.11b… Tháng 7-2003, IEEE phê chuẩn 802.11g. Chuẩn này sử dụng phương thức điều chế OFDM tương tự 802.11a nhưng lại dùng tần số 2,4GHz giống với chuẩn 802.11b. Chuẩn này vẫn đạt tốc độ 54Mbps và có khả năng tương thích ngược với chuẩn 802.11b nhưng không tương thích với chuẩn 802.11a. Vùng phủ sóng khoảng 38-40m. Chuẩn 802.11g phổ biến nhất hiện nay vùng phủ sóng khoảng 38-140m.

* Ưu điểm: Tốc độ cao, tầm phủ song tốt và ít bị che khuất.
* Nhược điểm: Giá thành đắt hơn 802.11b, có thể bị nhiễu bới các thiết bị khác sử dụng cùng băng thông.
  + 1. *IEEE 802.11n (Wifi 4)*

Đây là chuẩn được thiết kế để cải thiện tính năng của 802.11g về tổng băng thông được hỗ trợ bằng cách tận dụng nhiều tín hiệu không dây và anten (gọi là công nghệ MIMO (Multiple Input and Multiple Output). Khi chuẩn này hoàn thành, 802.11n sẽ hỗ trợ tốc độ lên đến 248 Mbps. 802.11n cũng cho tầm phủ sóng tốt hơn các chuẩn Wi-Fi trước đó nhờ

tăng cường độ tín hiệu. Các thiết bị 802.11n sẽ tương thích ngược với 802.11g, hoạt động trên cả hai tần số 2,4GHz và 5GHz. Vùng phủ sóng rộng khoảng 70-250m.

* Ưu điểm: Tốc độ nhanh, vùng phủ sóng tốt, trở kháng lớn hơn để chống nhiễu từ các tác động của môi trường.
* Nhược điểm: Chuẩn này vẫn chưa được ban bố, giá cao hơn 802.11g, sử dụng nhiều luồng tín hiệu có thể gây nhiễu với các thiết bị 802.11b/g kế cận.
  + 1. *IEEE 802.11ac (Wifi 5)*

Là chuẩn wifi mở rộng từ 802.11n, được sử dụng phổ biến hiện nay. Chuẩn sử dụng công nghệ băng tần kép, kết nối đông thời cả 2 băng tần 2,4GHz và 5GHz. 802.11ac cũng tương thích ngược với 802.11b/g/n. và băng thông đạt 1300Mbps trên 5GHz và 450Mbps trên 2,4GHz.

* Ưu điểm: tốc độ tối đa nhanh và phạm vi tín hiệu tốt hơn, khả năng chống nhiễu tốt hơn từ những nguồn bên ngoài.
* Nhược điểm: ít thiết bị hỗ trợ và giá thành cao
  + 1. *IEEE 802.11ax (Wifi 6)*

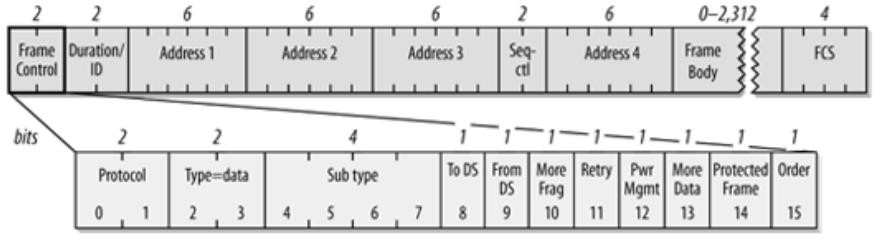
Đây là chuẩn không dây thế hệ tiếp theo, tốc độ nhanh hơn 802.11ac rất nhiều. Ngoài tốc độ, wifi 6 còn cung cấp hiệu suất tốt hơn trong các khu vực đông người như truongwf học hay doanh nghiệp… wifi 6 mang lại tốc độ 10Gbps và đạt tới 12Gbps ở khoảng cách rất ngắn.

Một tính năng nổi bật khác của chuẩn mới là OFDMA. OFDMA hiểu đơn giản là công nghệ giúp chia nhỏ các kênh truyền, sau đó ghép và truyền đến nhiều người dùng cùng một lúc. Từ đó tăng khả năng phục vụ đồng thời nhiều người dùng, giảm thiểu độ trễ, và tăng số lượng kết nối so với chuẩn WiFi 5. Công nghệ MU-MIMO trên WiFi 6 được nâng cấp hơn so với WiFi 5. Cụ thể MU-MIMO ở WiFi 6 hỗ trợ cả download và upload, trong khi ở WiFi 5 chỉ có MU-MIMO ở download. WiFi 6 đã được mở rộng băng thông tới 160 MHz, trong khi thế hệ WiFi 5 chỉ ở mức băng thông 80 MHz. Điều này giúp người dùng trải nghiệm tần số sóng của kênh rộng hơn, theo đó tận hưởng cảm giác xem video 8K cũng như tải các tập tin có dung lượng lớn về thiết bị đang bắt sóng WiFi đều không bị

giật lag. Wifi 6 ra đời kéo theo sự xuất hiện của WPA3, giao thức bảo mật không dây mới nhưng chưa hoàn thiện.

Cấu trúc frame:

Frame có thể chứa tối đa 2034 bytes dữ liệu.



* Trường Frame control: để xác định loại frame (frame quản lý, frame điều khiển, frame dữ liệu) và định hướng đường đi của frame từ thiết bị này sang thiết bị khác. Trường này chia làm nhiều trường nhỏ
* Protocol version: cho biết phiên bản của MAC
* Type: định dạng loại frame
* Subtype: kiểu con của frame điều khiển đang được truyền.
* To DS và From DS: cho biết liệu một khung dữ liệu được dành cho một hệ thống phân phối (hoặc một AP). Nếu cả hai trường được đặt thành 1, khung dữ liệu được truyền giữa các AP.
* More frag: cho biết một gói có được chia thành nhiều đoạn để truyền hay không.
* Retry: cho biết có truyền lại khung hay không. Trường này giúp loại bỏ các khung trùng lặp.
* Pwr Mgmt: cho biết chế độ quản lý năng lượng mong muốn của STA sau khi hoàn thành trao đổi khung, chẳng hạn như chế độ hoạt động hoặc ngủ.
* More data: chỉ ra rằng một AP truyền các gói có bộ đệm tới một STA ở chế độ tiết kiệm năng lượng.
* Protected Frame: cho biết liệu một khung có được mã hóa hay không.
* Order: cho biết liệu một khung có được truyền theo thứ tự hay không.
* Trường Duration: mang giá trị của Vectơ phân bổ mạng (NAV). Quyền truy cập vào phương tiện bị hạn chế trong thời gian do NAV quy định. Bất kỳ frame nào được truyền trong khoảng thời gian không có tranh chấp sẽ đặt trường Thời lượng thành 32,768. Các frame được truyền đến một đích quảng bá hoặc phát đa hướng (Địa chỉ 1 có tập bit nhóm) có thời lượng bằng 0. Nếu bit More Fragment trong trường Frame Control là 0, thì không còn phân mảnh trong frame, khi đó duration được đặt thành lượng thời gian cần thiết cho một không gian interframe ngắn và xác nhận phân đoạn.
* Frame sẽ được gửi từ thiết bị phát (transmitting device) đến thiết bị nhạn (receiving device). Vì vậy trong frame header address 1 luôn chứa RA (receiver address) và address 2 chứa TA (transmitter address). Trường address 3 chứa địa chỉ đích DA (destination address) khi RA không phải địa chỉ đích cuối hoặc chứa địa chỉ nguồn SA (source address) khi TA không phải địa chỉ nguồn mà frame được gửi. Trường address 4 sẽ không xuất hiện trừ khi 2 access point kết nối không dây với nhau.

## Cách bảo mật mạng WLAN không dây

* + 1. *Khoá WEP*

WEP là viết tắt của cụm từ Wired Equivalent Privacy. WEP được định nghĩa là một tiêu chuẩn bảo mật mạng không dây Wi-Fi. Từ đó, bạn có thể hiểu, khóa WEP là một loại mật mã bảo mật cho các thiết bị Wi-Fi. Các khóa WEP cho phép một nhóm các thiết bị trên mạng cục bộ trao đổi các thông điệp được mã hóa với nhau trong khi ẩn nội dung của các tin nhắn do người ngoài xem.

Có thể nói, khóa WEP là yếu tố cơ bản cho thuật toán mã hóa. Khóa WEP có thể được sử dụng theo 2 cách:

* + - Dùng để mã hóa dữ liệu
    - Dùng để định danh xác thực client
    1. *WPA (Wi-Fi Protected Access)*

WPA là giải pháp công nghệ thay thế cho WEP vốn có nhiều khuyết điểm. Một trong những cải tiến quan trọng của WPA là sử dụng hàm thay đổi khoá TKIP (Temporal Key Integrity Protocol) và kiểm tra tính toàn vẹn của thông tin (Message Integrity Check).

* + 1. *WPA2 (Wi-Fi Protected Access 2)*

WPA2 là phương thức bảo mật được thêm vào WPA dành cho các mạng không dây, nhằm cung cấp khả năng bảo vệ dữ liệu và kiểm soát truy cập mạng mạnh mẽ hơn. Nó cung cấp cho người dùng WiFi doanh nghiệp và tại gia đình mức độ đảm bảo cao rằng, chỉ những người dùng được ủy quyền mới có thể truy cập vào mạng không dây của họ.

Dựa trên tiêu chuẩn IEEE 802.11i, WPA2 cung cấp khả năng bảo mật cấp chính phủ bằng cách triển khai thuật toán mã hóa AES tương thích FIPS 140-2 của Viện Tiêu chuẩn và Công nghệ Quốc gia (NIST) FIPS 140-2, cùng xác thực dựa trên 802.1x.

Có hai phiên bản WPA2: WPA2-Personal và WPA2-Enterprise:

WPA2-Personal bảo vệ truy cập mạng trái phép bằng cách sử dụng mật khẩu đã thiết lập.

WPA2-Enterprise xác minh người dùng mạng thông qua một server. WPA2 tương thích ngược với WPA.

Lỗ hổng được phát hiện trong giao thức WPA2

Vào ngày 16 tháng 10 năm 2017, các nhà nghiên cứu bảo mật đã tiết lộ lỗ hổng có mức độ nghiêm trọng cao trong giao thức WPA2, khiến những kẻ tấn công có thể nghe trộm lưu lượng WiFi đi qua giữa các máy tính và những điểm truy cập.

Cuộc tấn công exploit Proof-Of-Concept được gọi là KRACK (Key Reinstallation Attacks) ảnh hưởng đến chính giao thức WPA2 cốt lõi và có hiệu quả đối với các thiết bị chạy hệ điều hành Android, Linux, Apple, Windows và OpenBSD, cũng như MediaTek Linksys và nhiều loại hệ điều hành khác chạy trên các thiết bị. Sau đó, các nhà cung cấp đã cung cấp bản vá và cập nhật cho người dùng để khắc phục lỗ hổng này.

* + 1. *WPA3 (Wi-Fi Protected Access 3)*

Wi-Fi Alliance đã công bố giao thức bảo mật WPA3 vào năm 2018, cung cấp một phương pháp an toàn và đáng tin cậy hơn nhiều thay thế WPA2 và các giao thức bảo mật cũ hơn. Những thiếu sót cơ bản của WPA2 như bắt tay bốn chiều không hoàn hảo và sử dụng PSK (khóa chia sẻ trước) khiến kết nối Wi-Fi của bạn dễ bị xâm phạm. WPA3 có những cải tiến bảo mật hơn nữa giúp khó xâm nhập vào mạng bằng cách đoán mật khẩu. Dưới đây là các cân nhắc triển khai được khuyến nghị:

## Bảo vệ mật khẩu đáng tin cậy

WPA3-Enterprise được kéo dài mã hóa thành 192 bit (mã hóa 128 bit ở chế độ WPA3-Personal) để tăng cường độ mạnh của mật khẩu. Nó bảo vệ chống lại các mật khẩu yếu có thể bị bẻ khóa tương đối dễ dàng thông qua việc đoán.

## Bảo vệ các thiết bị mạng

WPA3 thay thế Khóa chia sẻ trước WPA2 (WPA2 Pre-Shared Key - PSK) bằng Xác thực đồng thời - Simultaneous Authentication of Equals (SAE) để tránh các cuộc tấn công cài đặt lại khóa như KRACK khét tiếng. Nó sẽ giữ an toàn cho các thiết bị mạng của bạn trong khi kết nối với điểm truy cập không dây. tấn công từ điển ngoại tuyến.

## Kết nối an toàn hơn trên khu vực công cộng

Cho dù kẻ tấn công có được khóa mã hóa lưu lượng, thật khó để tính toán mức sử dụng lưu lượng và dữ liệu được truyền bằng WPA3-Personal. SAE mang lại lợi ích của bảo mật chuyển tiếp (forward-secrecy) và bảo mật dữ liệu hơn nhiều so với mạng mở. WPA3 cũng cung cấp các khung quản lý được bảo vệ (Protected management frames - PMF) để tránh nghe lén và giả mạo từ khu vực công cộng.

## Frame Relay

* 1. **Khái niệm**

Frame Relay là một dịch vụ truyền số liệu mạng diện rộng dựa trên công nghệ chuyển mạch gói. Đây là một chuẩn của CCITT và ANSI định ra quá trình truyền dữ liệu qua mạng dữ liệu công cộng. Hiện tại Frame Relay phục vụ cho các khách hàng có nhu cầu kết nối các mạng diện rộng và sử dụng các ứng dụng riêng với tốc độ kết nối cao (băng thông tối đa là 44,736 Mbit/s) và phục vụ cho các ứng dụng phức tạp như tiếng nói, âm thanh và hình ảnh. Đặc điểm của Frame Relay là truyền thông tin qua mạng diện rộng bằng việc chia dữ liệu thành những gói tin. Mỗi gói tin đi qua một dãy các thiết bị chuyển mạch trong mạng Frame Relay để đi đến đích.

Đối với hầu hết các dịch vụ, mạng cung cấp một mạch ảo vĩnh viễn (PVC). Điều đó có nghĩa là khách hàng nhận thấy một kết nối liên tục, chuyên dụng mà không phải trả tiền cho kênh thuê riêng toàn thời gian. Nhà cung cấp dịch vụ tìm ra cách định tuyến từng frame đến đích của nó và tính phí dựa trên việc sử dụng. Ngược lại, các mạch ảo chuyển

mạch (SVC) là các kết nối tạm thời bị phá hủy sau khi hoàn thành một quá trình truyền dữ liệu cụ thể.

## Cấu trúc khung của Frame relay

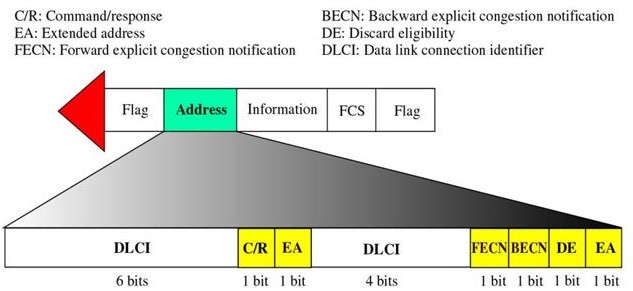


*Hình 16. Cấu trúc khung của Frame relay.*

Cờ F (Flag) gồm 1 byte dẫn đầu và 1 byte dành cho cờ F để kết thúc. Cả 2 byte cờ Flag luôn có giá trị là: 01111110.

Address (2 byte) để biết khung chuyển đến đâu.

Trường I (Information) dành cho dữ liệu thông tin có nhiều byte.



*Hình 17. Cấu trúc trường Address.*

DLCI: đánh số DLCI gói frame

C/R (Command/Response): dùng để hỏi đáp

EA: nếu EA=1 thì 4 bit DLCI tiếp theo được dùng tới DE: nếu DE=1 thì mạng có thể bỏ frame nếu mạng nghẽn

FECN: thông báo độ nghẽn phía thu BECN: thông báo độ nghẽn phía phát

2 byte cho việc kiểm tra khung – FCS (Frame Check Sequence) để phân tích và biết được các gói thiếu, đủ, đúng hay sai. Trên cơ sở đó, nó sẽ trả lời cho phía phát biết.

## Cách thức hoạt động

Đối với WAN chuyển tiếp frame để gửi dữ liệu, cần phải có thiết bị đầu cuối dữ liệu (DTE) và thiết bị kết cuối mạch dữ liệu (DCE). DTE thường được đặt tại cơ sở của khách hàng và có thể bao gồm thiết bị đầu cuối, bộ định tuyến, cầu nối và máy tính cá nhân. Các nhà cung cấp dịch vụ quản lý DCE, cung cấp dịch vụ chuyển mạch và các dịch vụ khác.

Frame relay dựa trên công nghệ chuyển mạch gói X.25 cũ hơn được thiết kế để gửi dữ liệu tương tự như hội thoại. Tuy nhiên, không giống như X.25, frame relay là một công nghệ gói tin nhanh. Điều đó có nghĩa là giao thức không cố gắng sửa lỗi. Khi một lỗi được phát hiện trong một khung, nó chỉ đơn giản là bị loại bỏ. Các điểm cuối chịu trách nhiệm phát hiện và truyền lại các khung bị rớt. Tỷ lệ lỗi trong mạng kỹ thuật số là nhỏ so với mạng tương tự.

Frame relay thường được sử dụng để kết nối các mạng LAN với các đường trục chính. Nó cũng được sử dụng trên các mạng WAN công cộng và trong các môi trường mạng riêng với các đường truyền T-1 cho thuê. Nó cần một kết nối chuyên dụng trong quá trình truyền và không lý tưởng cho thoại hoặc video, những thứ cần một luồng truyền ổn định. Frame relay sẽ gửi các gói ở lớp data link của mô hình OSI, chứ không phải ở lớp network. Một khung có thể kết hợp các gói từ các giao thức khác nhau như Ethernet và

X.25. Nó có kích thước thay đổi và có thể lớn đến một nghìn byte hoặc hơn.

Frame relay sử dụng các mạch ảo tạm thời để gửi các gói qua mạng thông qua các chuyển mạch frame relay thay vì gửi trực tiếp qua các giao diện vật lý của mạng. ISP đảm bảo một mức băng thông nhất định cho một mạch ảo hoạt động trong điều kiện bình thường. Các loại mạch ảo gồm mạch ảo vĩnh viễn (PVC) và mạch ảo chuyển mạch (SVC).

PVC dành cho các kết nối phải được duy trì trong thời gian dài, ngay cả khi dữ liệu không được truyền. SVC dành cho các kết nối tạm thời chỉ kéo dài trong một phiên duy nhất. Các

SVC được thành lập theo từng phiên và các PVC được thành lập trước. PVC cung cấp một mức độ dịch vụ được thiết lập trước, điều này làm cho chúng trở nên đáng tin cậy hơn. SVC thì rẻ hơn, bởi vì chúng sử dụng bất kỳ tài nguyên mạng nào có sẵn.

Mỗi kết nối PVC ở cuối mỗi thiết bị đầu cuối được xác định bằng một địa chỉ có chiều dài 10 bit trong phần header đầu của frame, còn được gọi là DLCI. DLCI thường được dùng để ánh xạ đến địa chỉ lớp mạng của đích đến, tức địa chỉ L3 của router ở đầu xa của mạch PVC. Sau đó dữ liệu cần được truyền trên hạ tầng Frame relay sẽ được đóng gói trong các header này. Mỗi header trong Frame Relay được chèn vào giá trị DLCI tương ứng đến địa chỉ lớp mạng của đích đến. Các frame sau đó sẽ được gửi đến tổng đài với giá trị DLCI ban đầu. Các frame này tiếp tục được trung chuyển về phía mạng đích thông qua các tổng đài trung gian của các nhà cung cấp dịch vụ FR. Mỗi header trong Frame Relay được chèn vào giá trị DLCI tương ứng đến địa chỉ lớp mạng của đích đến. Các frame sau đó sẽ được gửi đến tổng đài với giá trị DLCI ban đầu. Các frame này tiếp tục được trung chuyển về phía mạng đích thông qua các tổng đài trung gian của các nhà cung cấp dịch vụ FR. DLCI có thể được đánh số tự động bằng LMI.

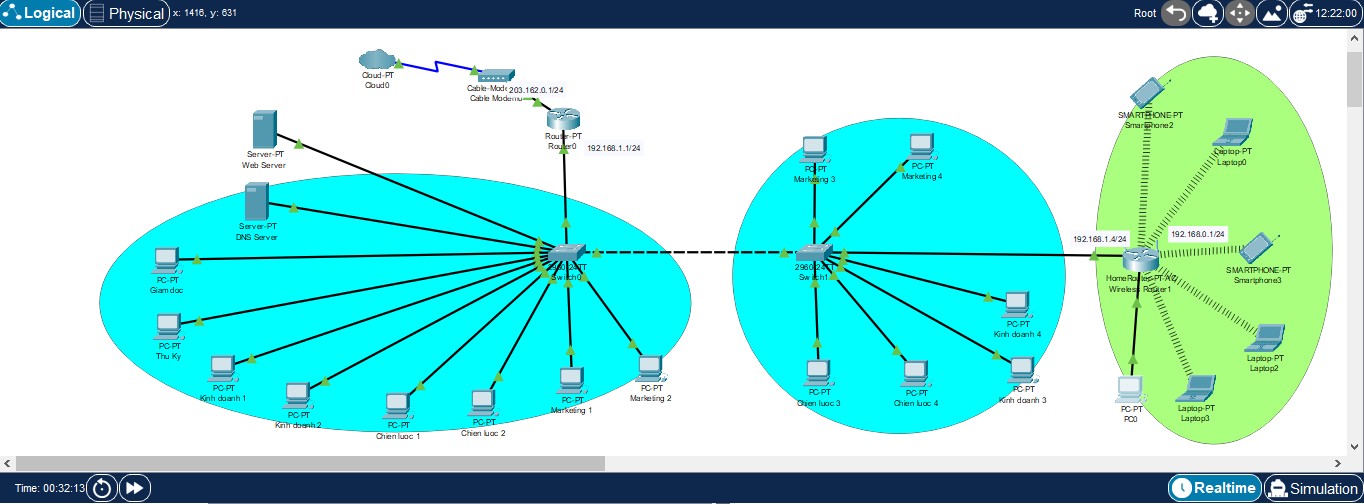
## Ưu điểm và nhược điểm của Frame relay

Ưu điểm:

* + - Không thực hiện sửa lỗi gây tốn thời gian và tài nguyên mạng.
    - Rẻ hơn các dòng chuyên dụng và yêu cầu ít phần cứng hơn.
    - Linh hoạt: nó sử dụng số nhận dạng kết nối liên kết dữ liệu (DLCI). DLCI là số xác định mạch logic giữa bộ định tuyến và công tắc chuyển tiếp khung.
    - Độ trễ thấp: nó ít bị trễ hơn vì các thành phần mạng khác xử lý sửa lỗi. Nhược điểm:
    - Mạng phải có sẵn để nó được sử dụng đúng cách.
    - Do tính chất nối mạng của chuyển tiếp khung, một nhược điểm khác là tốc độ chậm có thể xảy ra nếu quá nhiều kết nối đang sử dụng cùng một trạm.

# PHẦN HAI: MÔ PHỎNG MẠNG ETHERNET, WIRELESS LAN VÀ FRAME RELAY

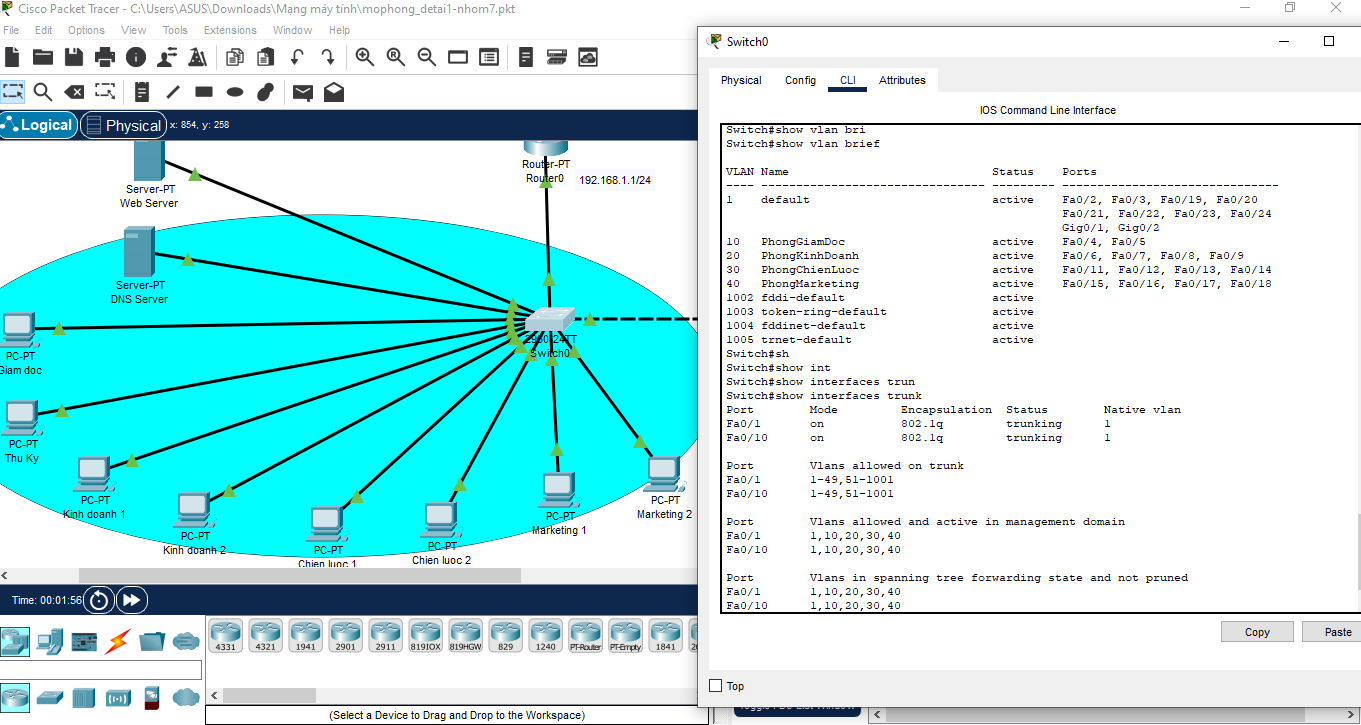
## Mô phỏng mạng Ethernet



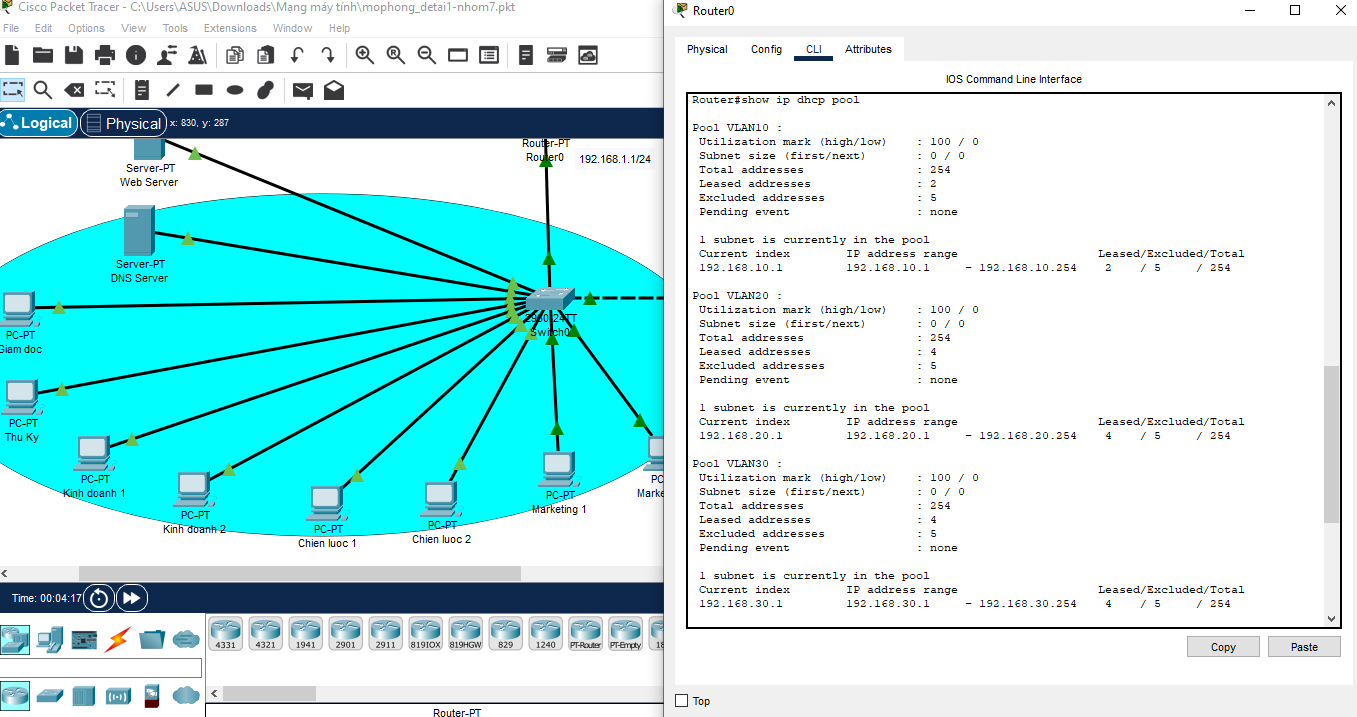
*Hình 18. Topology của mạng mô phỏng*

Mạng trên gồm LAN và WLAN, mạng LAN được chia thành các VLAN là: VLAN10 192.168.10.0/24, VLAN20 192.168.20.0/24, VLAN30 192.168.30.0/24 ứng với

các phòng ban, VLAN40 192.168.40.0. có router làm DHCP server cấp IP động cho từng VLAN.



Hình : Cấu hình VLAN



Hình : Cấu hình DHCP server cho từng VLAN

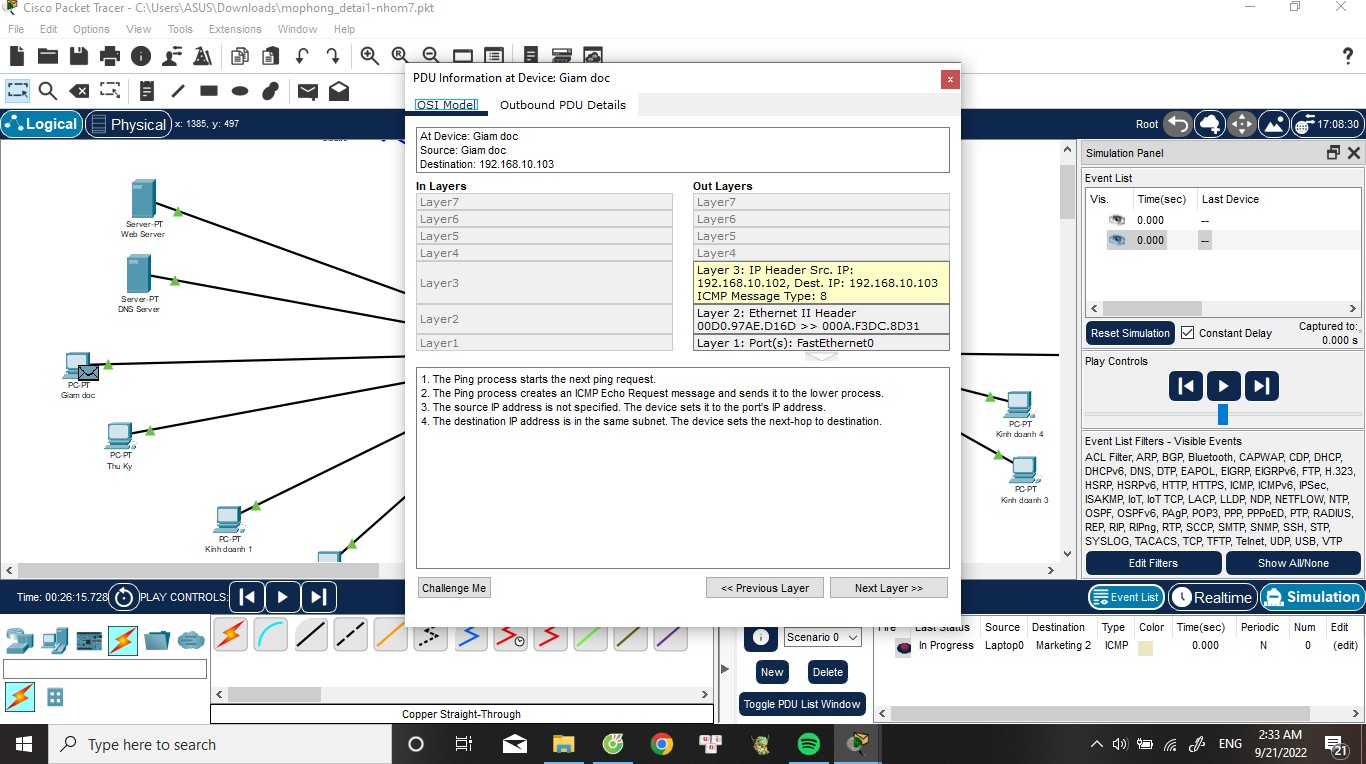
Mô phỏng khi ping từ PC Giam doc tới PC Thu Ky.

Ta có thấy các thông tin của gói tin:

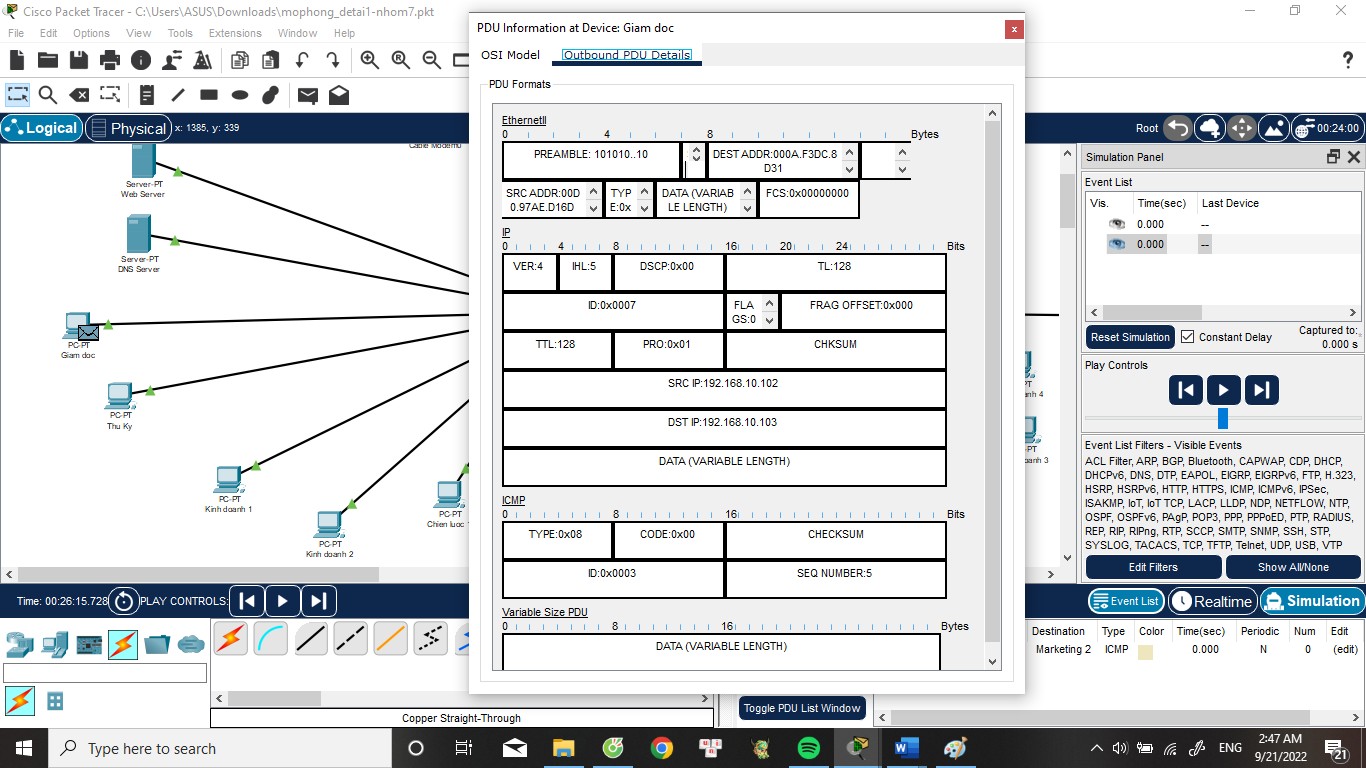
Ở lớp 3: IP nguồn 192.168.10.102, IP đích 192.168.10.103.

Ở lớp 2: MAC nguồn 00d0.97ae.d16d của PC Giam doc, MAC đích 000a.f3dc.8d31 của PC Thu Ky, khung được đóng theo chuẩn Ethernet II (DIX). Trường Kiểu chỉ ra kiểu của dữ liệu là IPv4 (0x0800).

Ở lớp 1: Gói tin được đưa ra cổng FastEthernet0

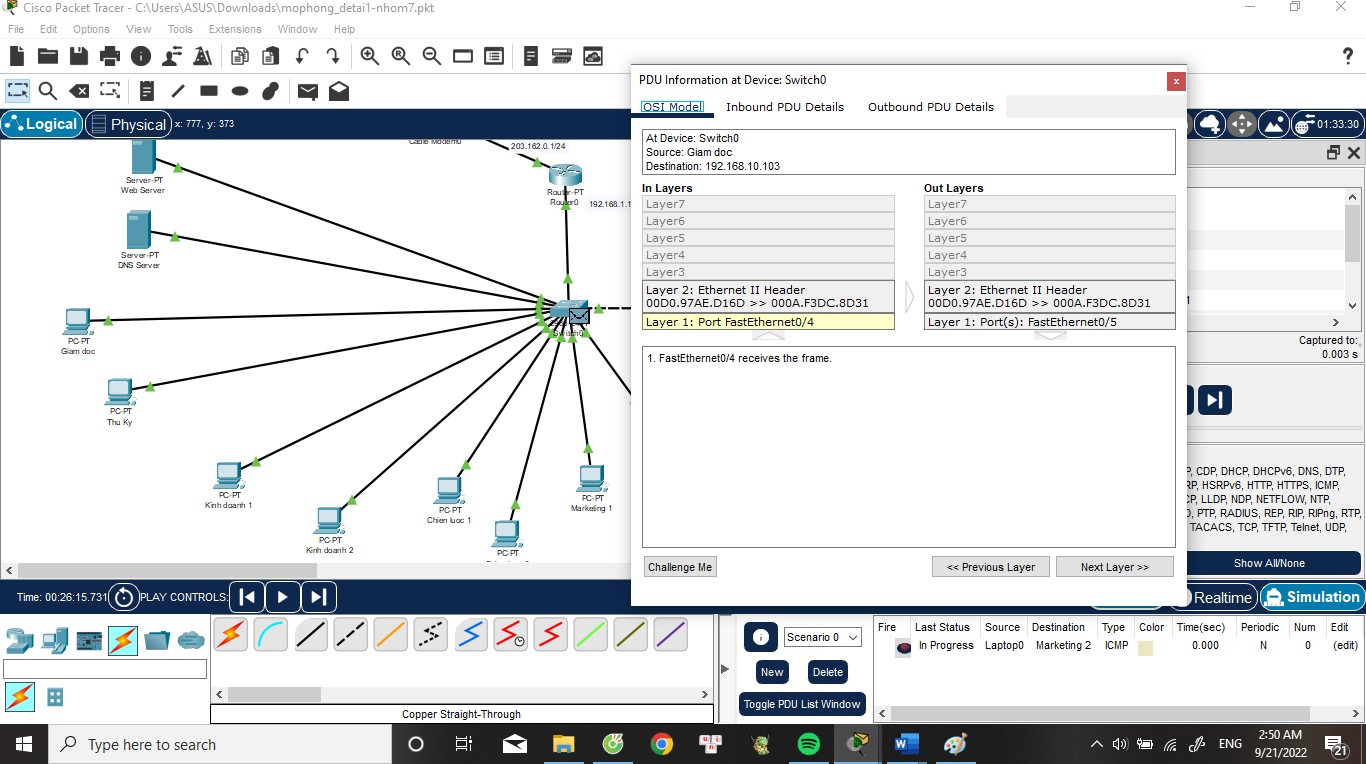


*Hình 19. Gói tin bắt đầu từ PC Giam doc: Mô hình OSI.*



*Hình 20. Gói tin bắt đầu từ PC Giam doc: Dạng khung dữ liệu.*

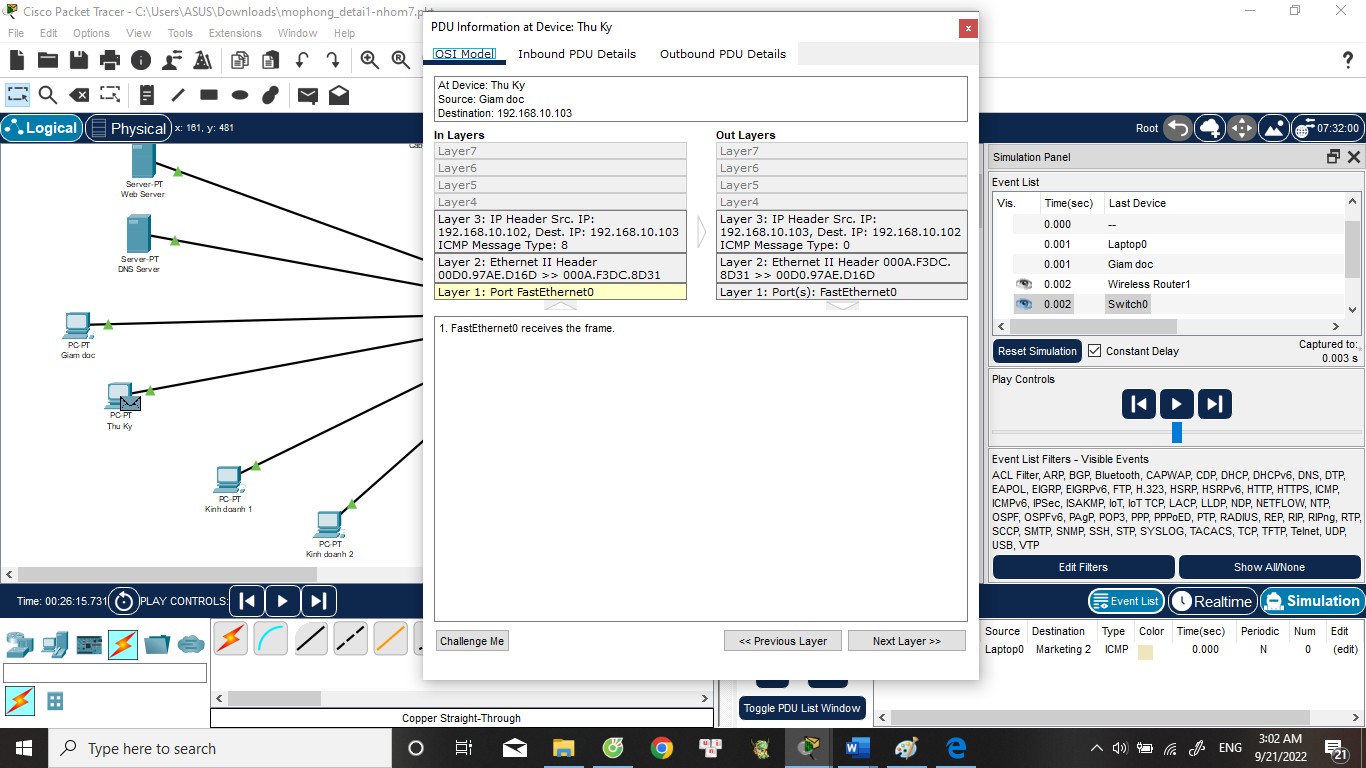
Gói tin được gửi đến Switch và Switch sẽ dựa vào bảng địa chỉ MAC để đưa gói tin đến đúng nơi.



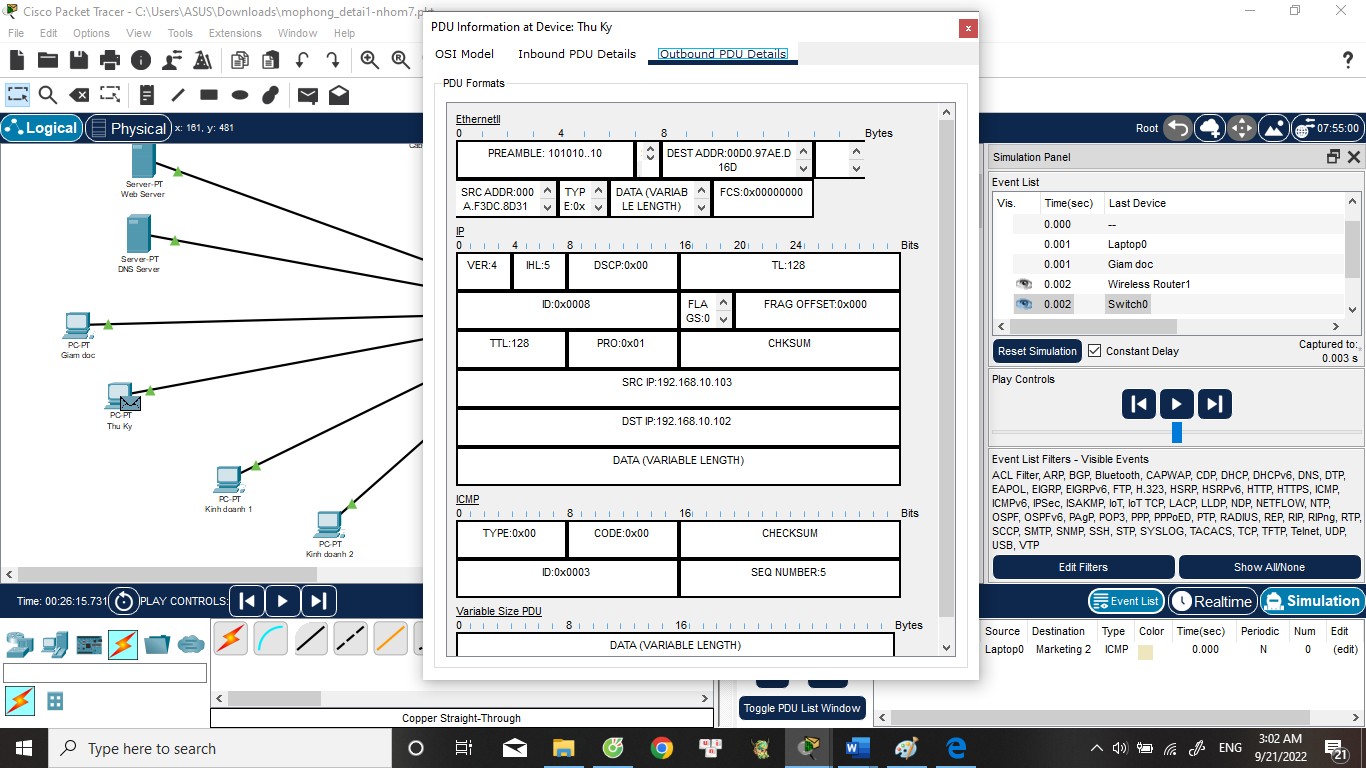
*Hình 21. Gói tin được gửi đến Switch.*

Sau khi gói tin từ PC Giam doc được gửi đến, PC Thu Ky cũng gửi lại gói tin phản

hồi.

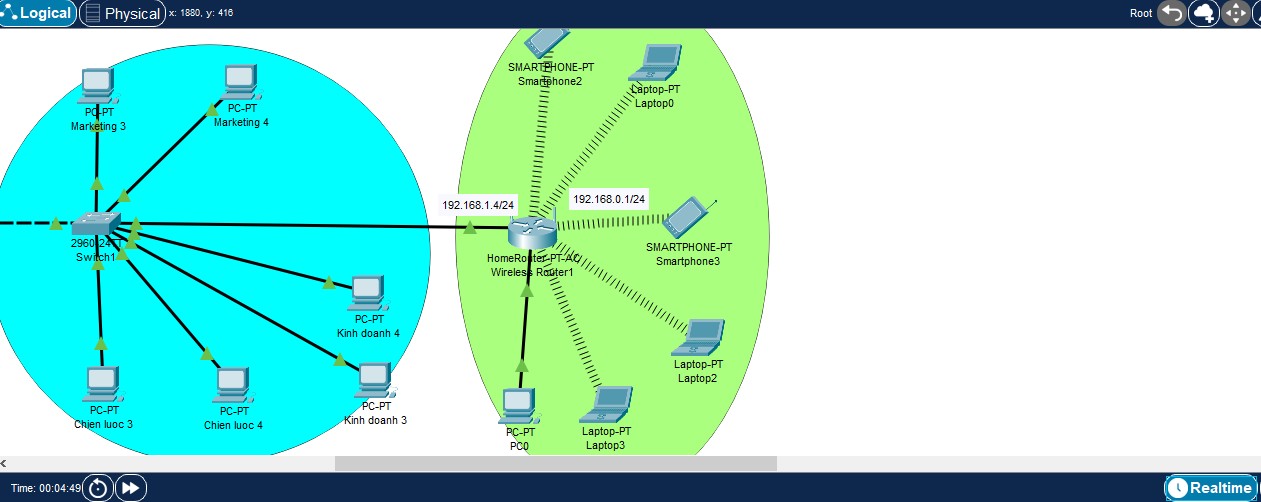


*Hình 22. Gói tin phản hồi từ PC Thu Ky: Mô hình OSI*

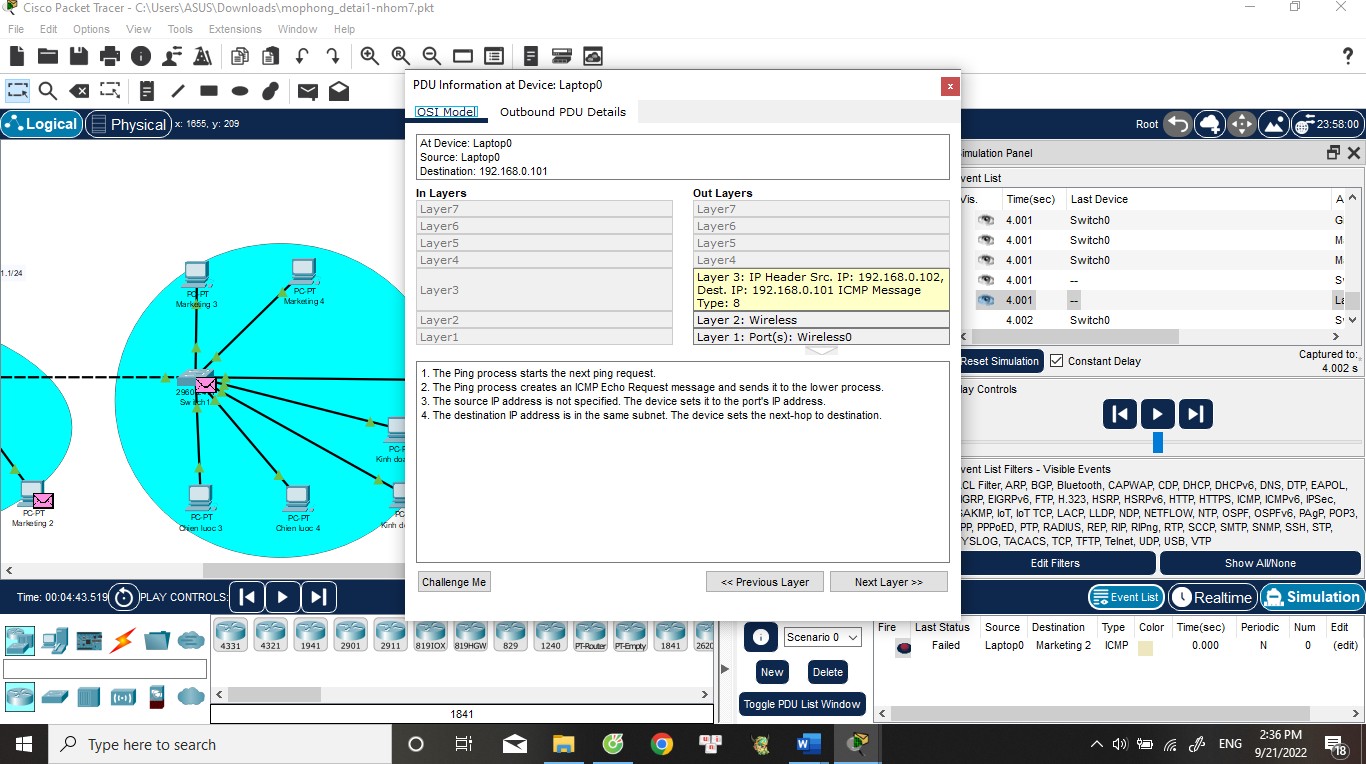


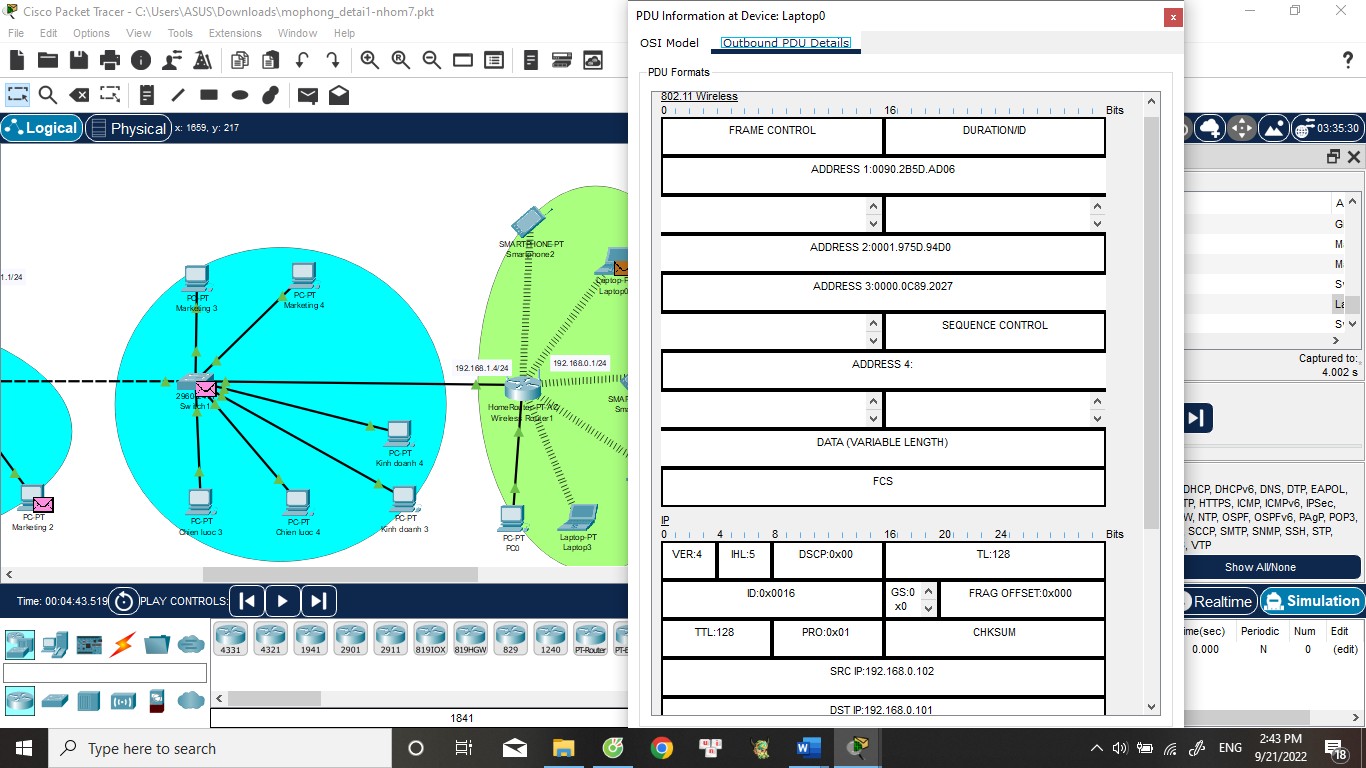
*Hình 23. Gói tin phản hồi từ PC Thu Ky: Dạng khung dữ liệu.*

## Mô phỏng Wireless

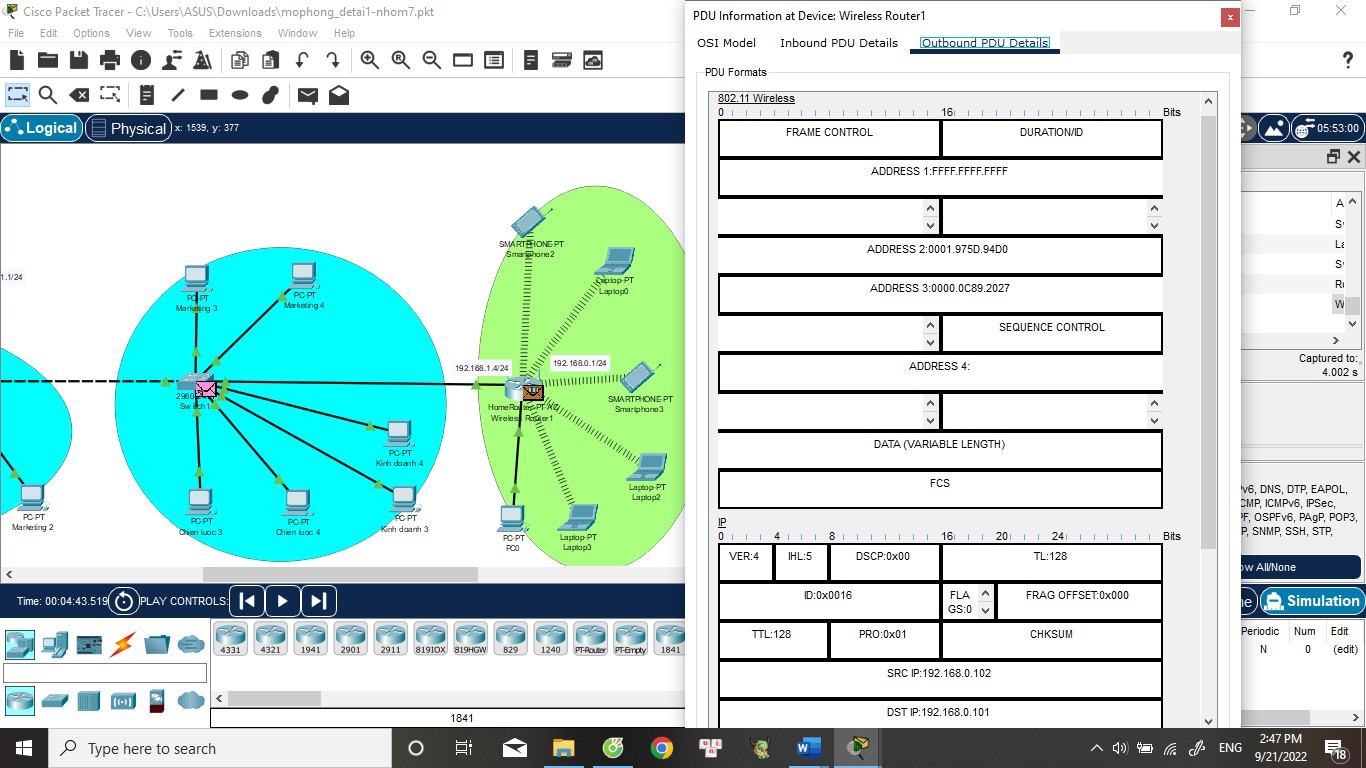


*Hình 24. Ping từ Laptop0 đến Laptop3*



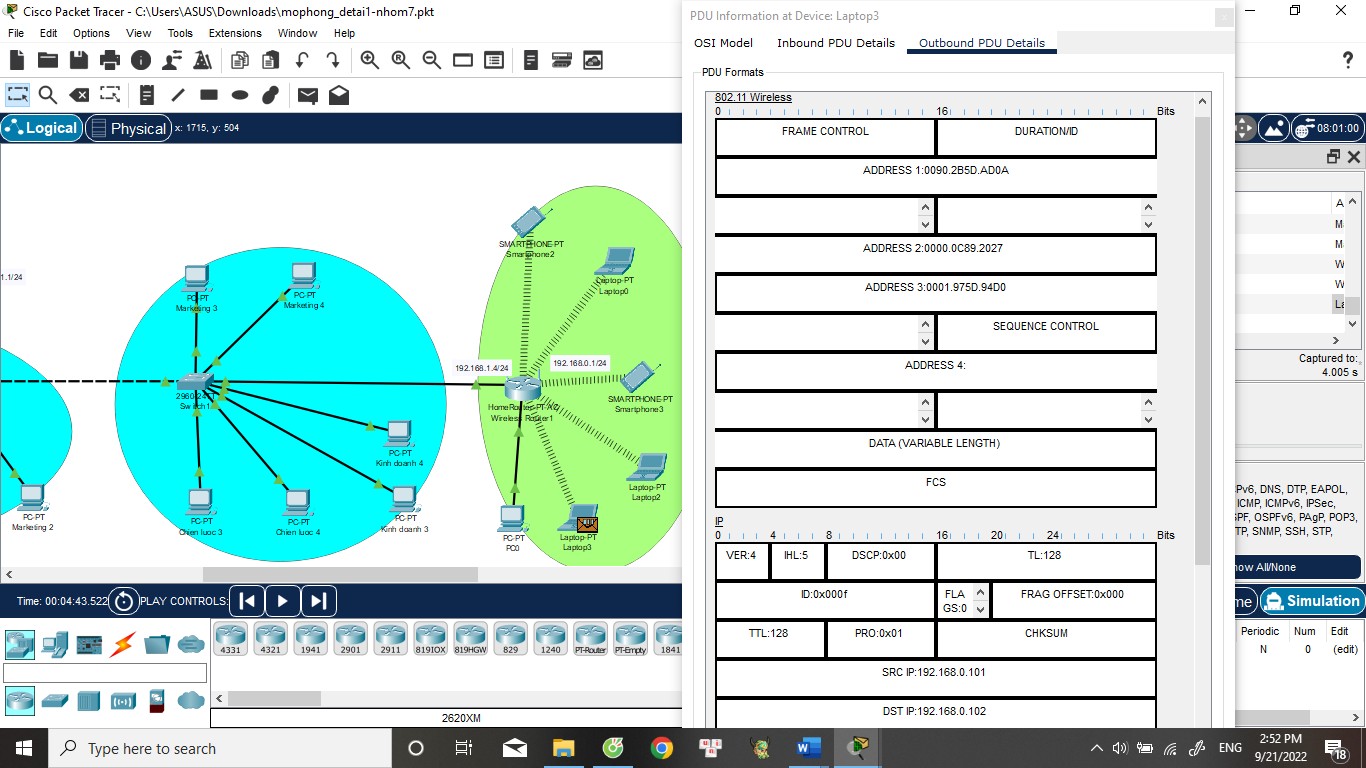


*Hình 25. Gói tin chuẩn bị gửi từ Laptop0.*



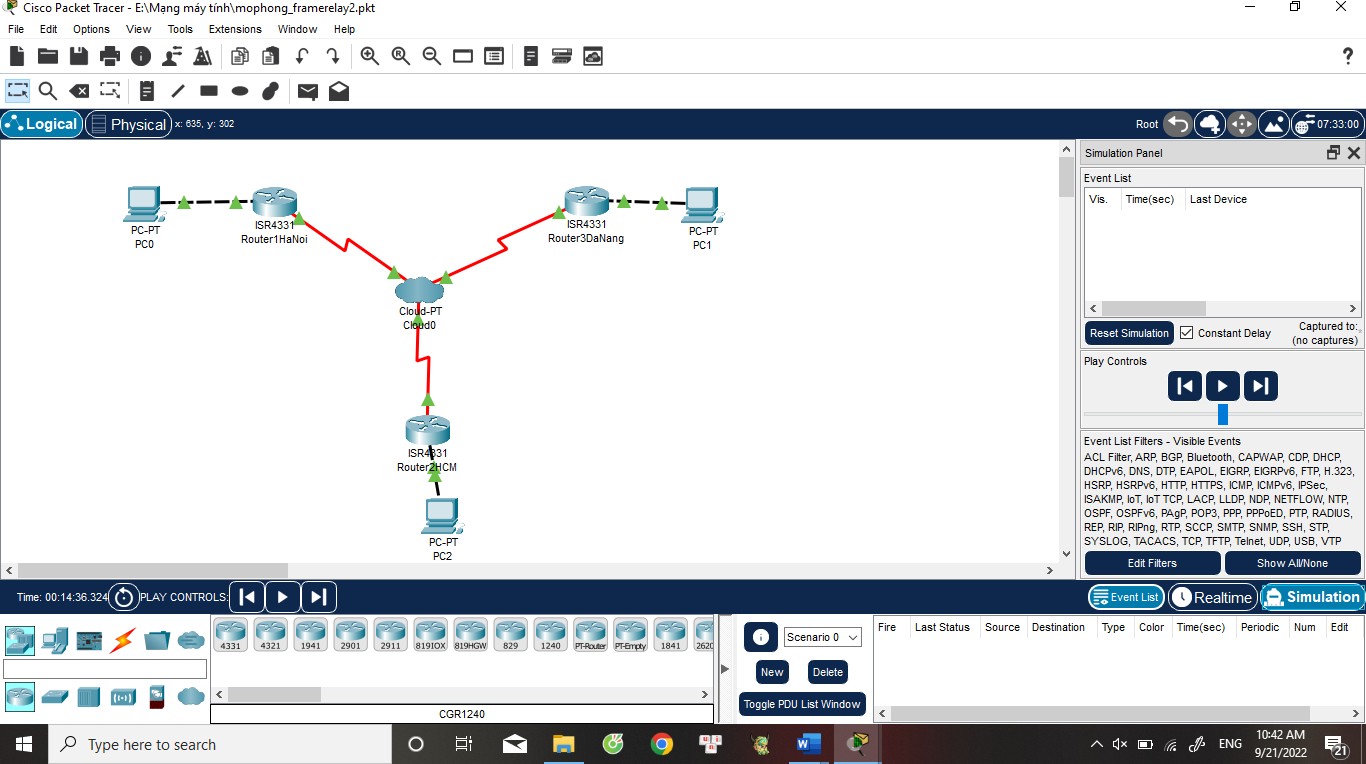
*Hình 26. Gói tin ở Wireless Router.*

Laptop 3 nhận được gói tin và phản hồi lại Laptop0



*Hình 27. Gói tin phản hồi lại Laptop0*

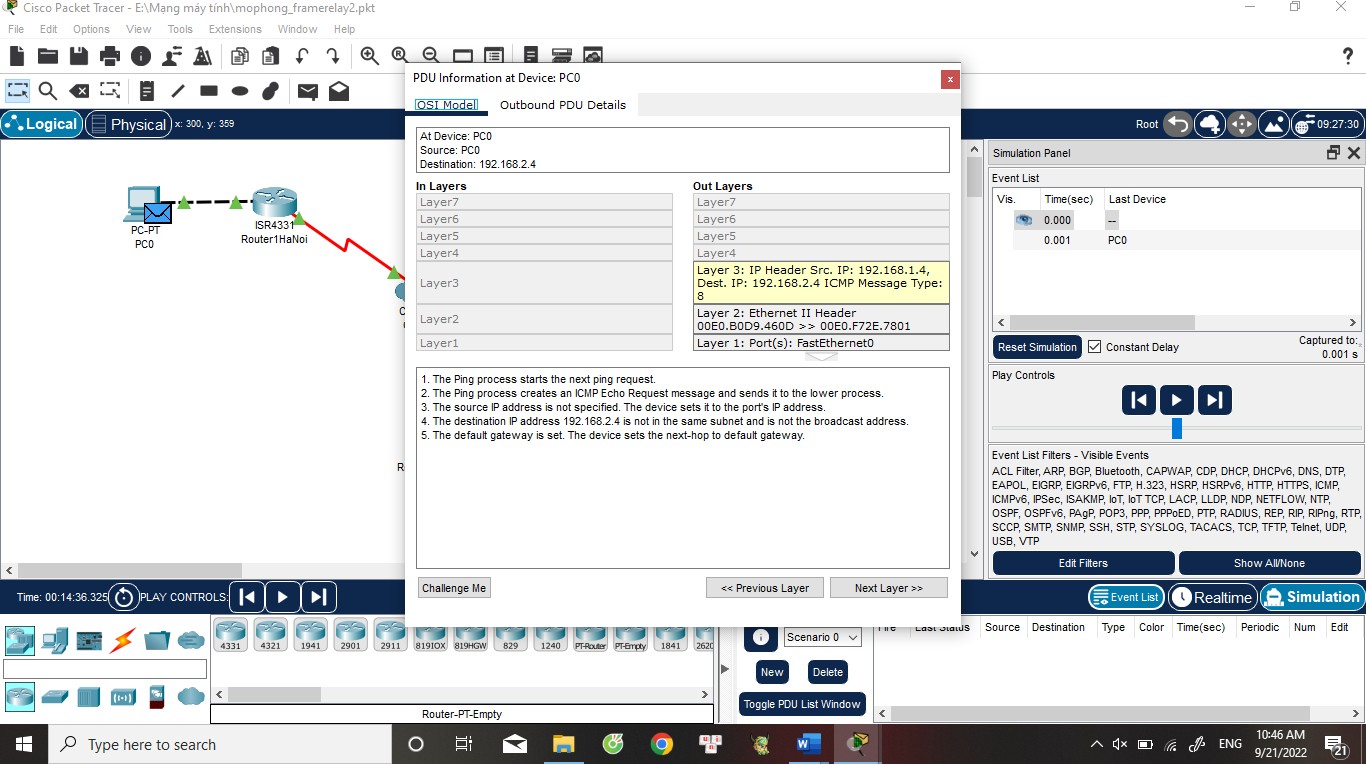
## Mô phỏng Frame Relay



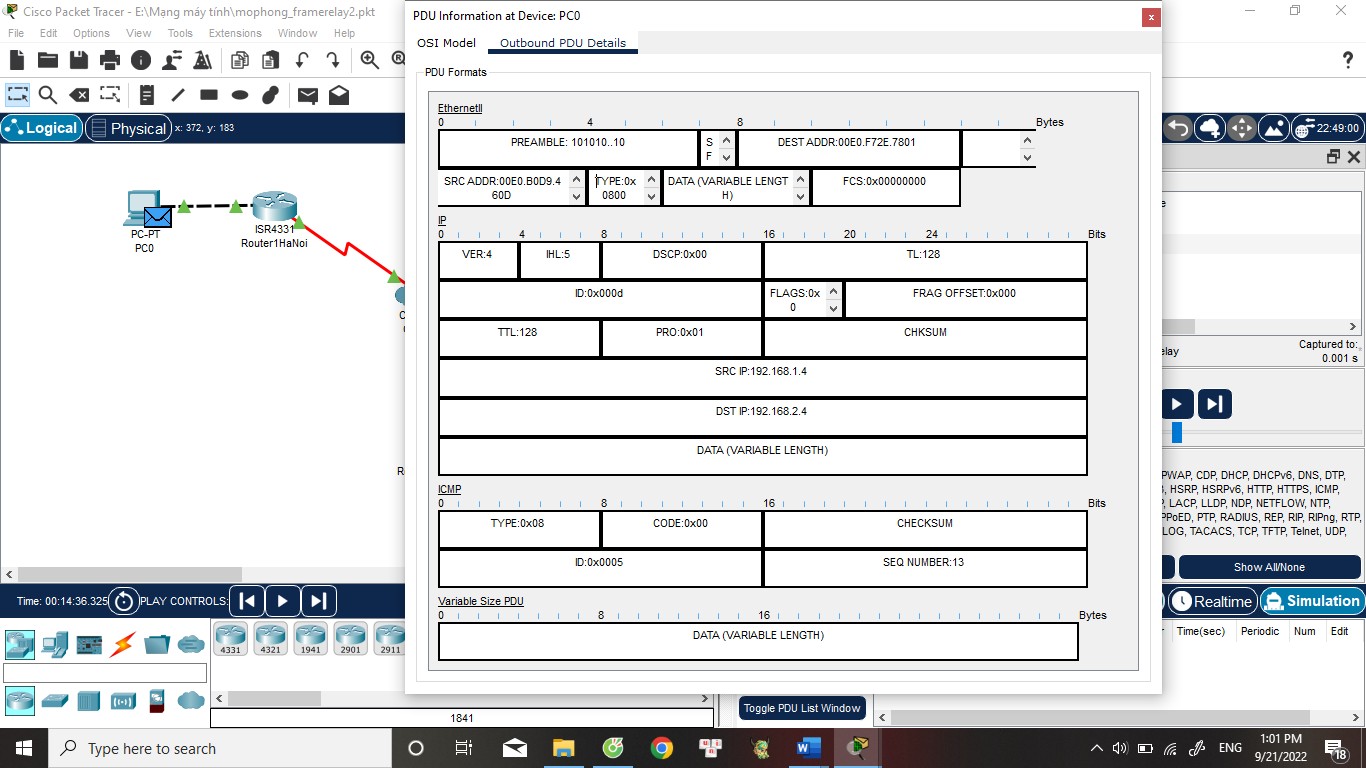
*Hình 28. Mô hình mạng mô phỏng Frame Relay.* Quan sát khi ping từ PC ở Hà Nội đến PC ở TP Hồ Chí Minh. Ở lớp 3: IP nguồn 192.168.1.4, IP đích 192.168.2.4.

Ở lớp 2: địa chỉ MAC nguồn 00e0.b0d9.460d của port FastEthernet0 của PC0, địa chỉ MAC đích 00e0.f72e.7801 của router1 ở Hà Nội. Khung được đóng theo chuẩn Ethernet II, trường Kiểu cho thấy dữ liệu của giao thức IPv4 (0x0800).

Ở lớp 1: Gói tin được đưa ra cổng FastEthernet0



*Hình 29. Gói tin ở PC0 chuẩn bị được gửi đi: Mô hình OSI.*



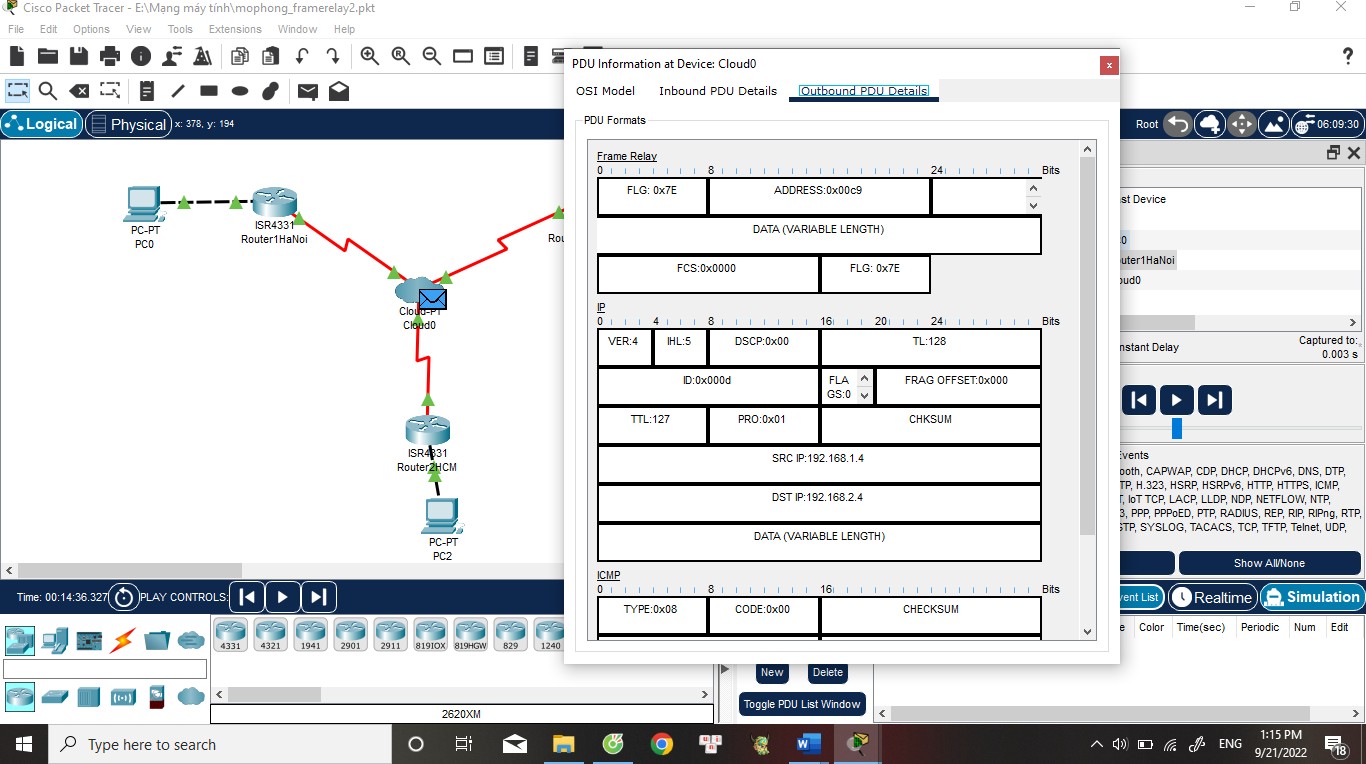
*Hình 30. Gói tin ở PC0 chuẩn bị được gửi đi: Dạng khung dữ liệu.*

Gói tin được gửi qua router và được đóng gói theo Frame relay, trường Địa chỉ cho biết DLCI là 102 (0x0066) ở đây nghĩa là gói tin từ Router1 ở Hà Nội gửi qua Router2 ở TP Hồ Chí Minh.



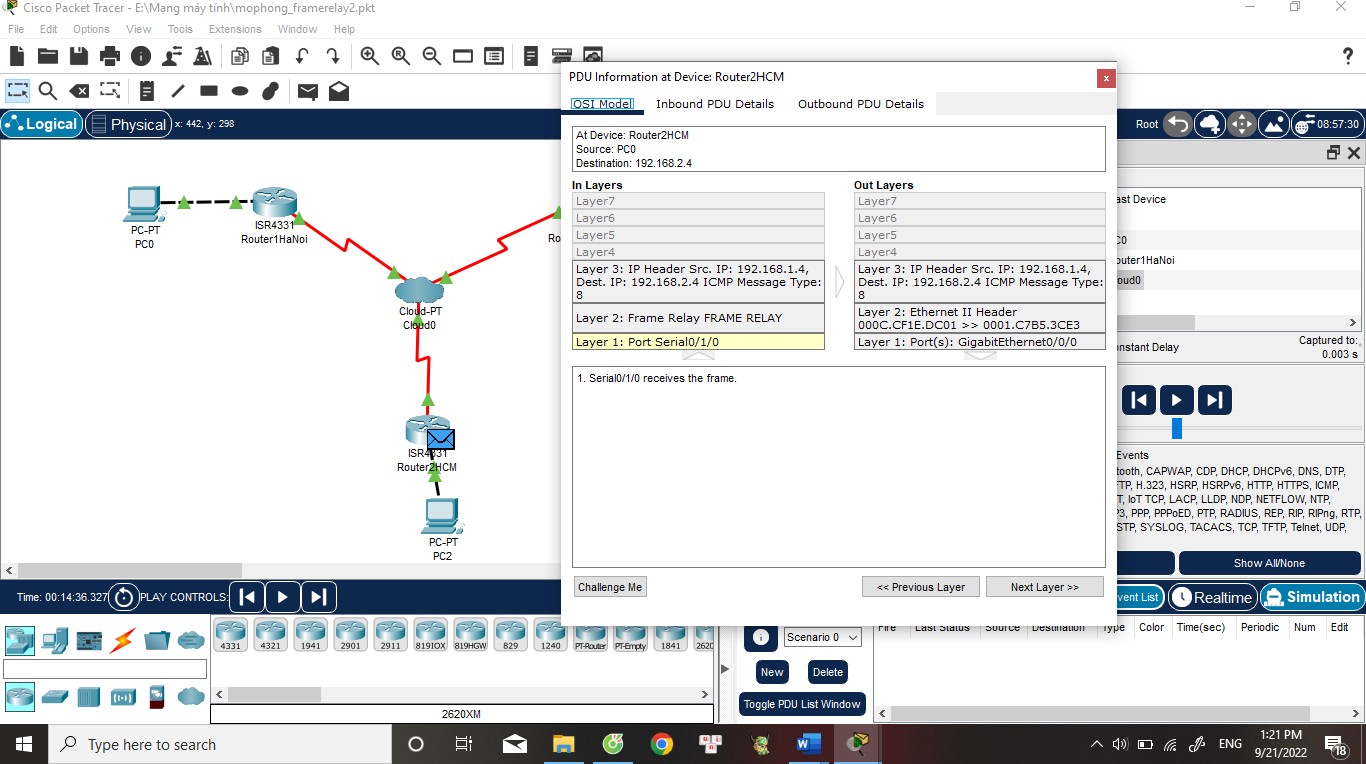
*Hình 31. Gói tin ở Router1 Hà Nội.*

Ở Cloud0 gói tin sẽ tiếp tục được chuyển qua pvc có DLCI 201 để đến được router2 ở TP Hồ Chí Minh nên DLCI trong khung của Frame relay được đổi thành 201 (0x00c9)



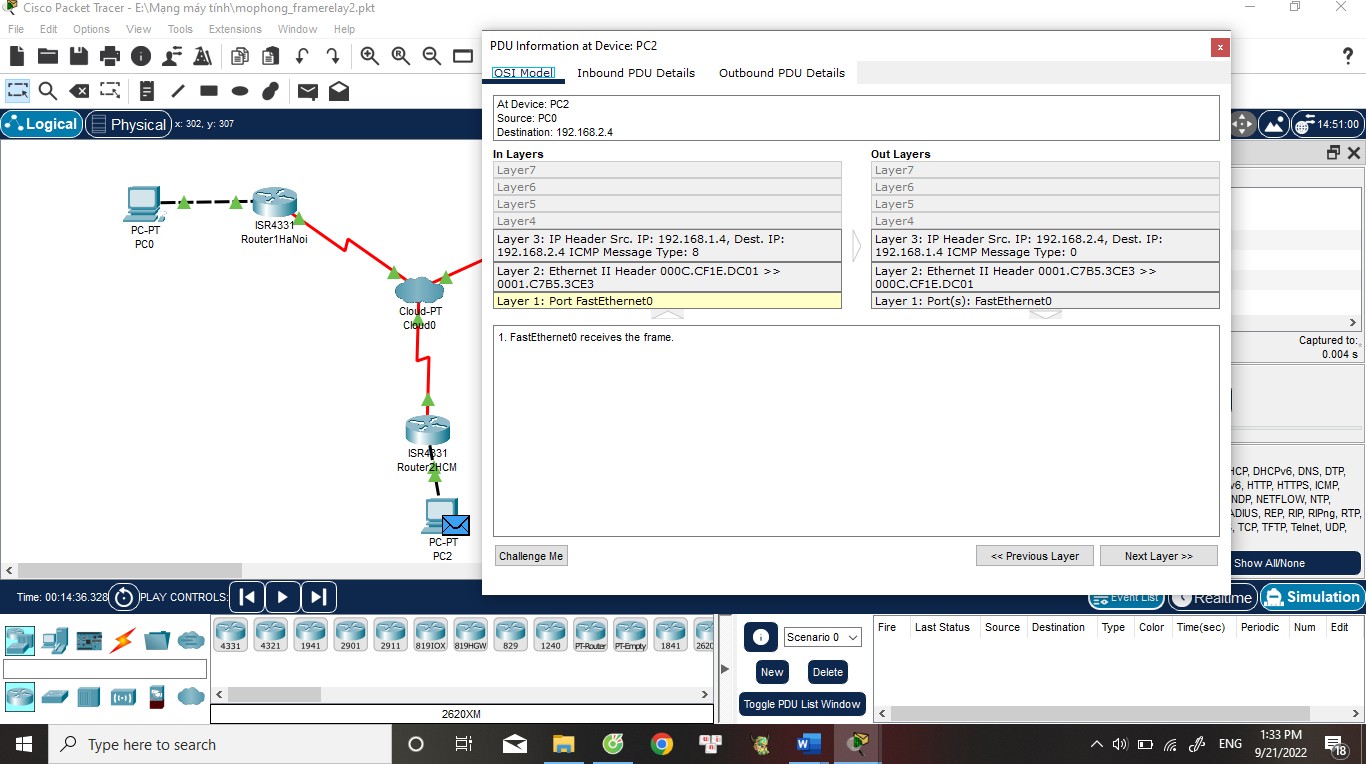
*Hình 32. Gói tin ở Cloud0.*

Gói tin được gửi vào cổng Serial0/1/0 của router2 và được chuyển qua cổng GigabitEthernet0/0/0 địa chỉ MAC 000c.cf1e.dc01 để đến PC2 địa chỉ MAC 001.c7b5.3ce3.

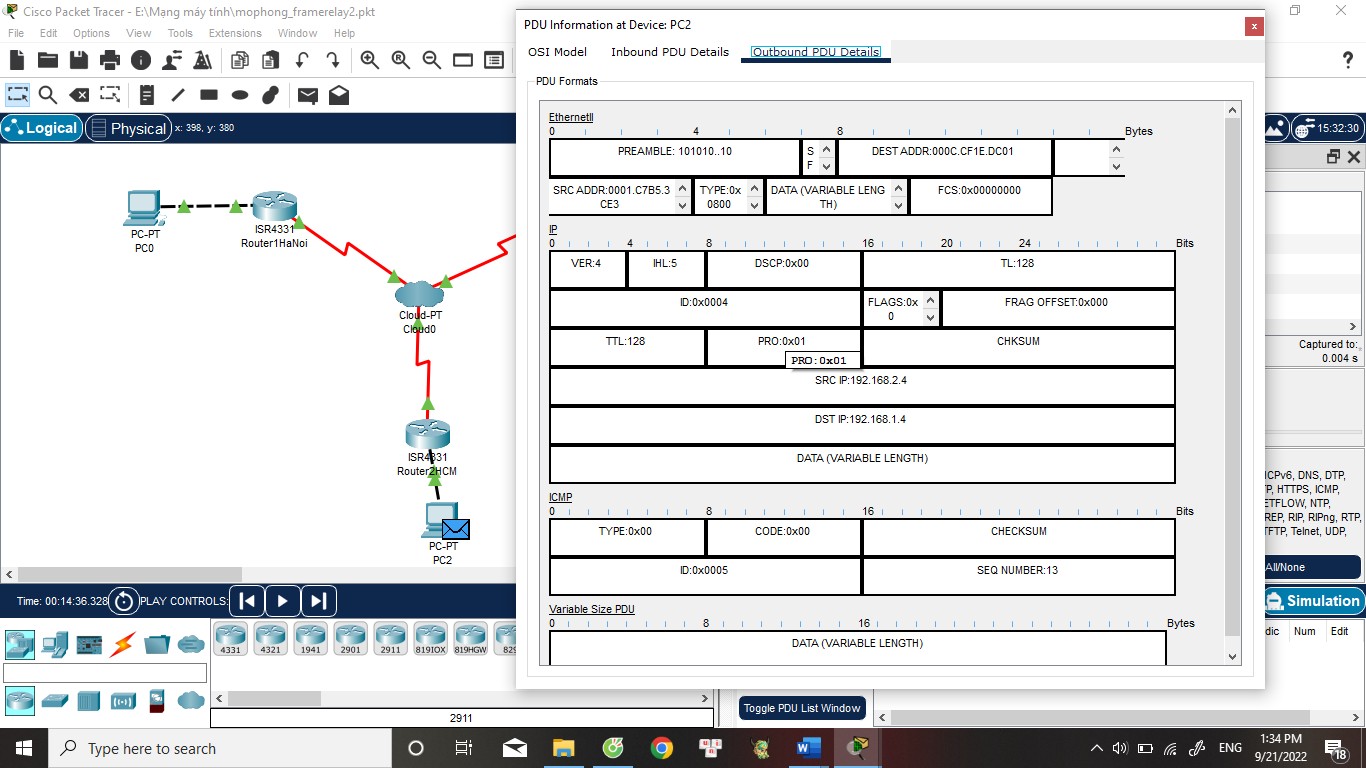


*Hình 33. Gói tin ở Router2 TP. Hồ Chí Minh.*

PC2 cũng chuẩn bị một gói tin phản hồi gửi lại PC0.



*Hình 34. Gói tin phản hồi của PC2 về PC0: Mô hình OSI.*



*Hình 35. Gói tin phản hồi của PC2 về PC0: Dạng khung dữ liệu.*