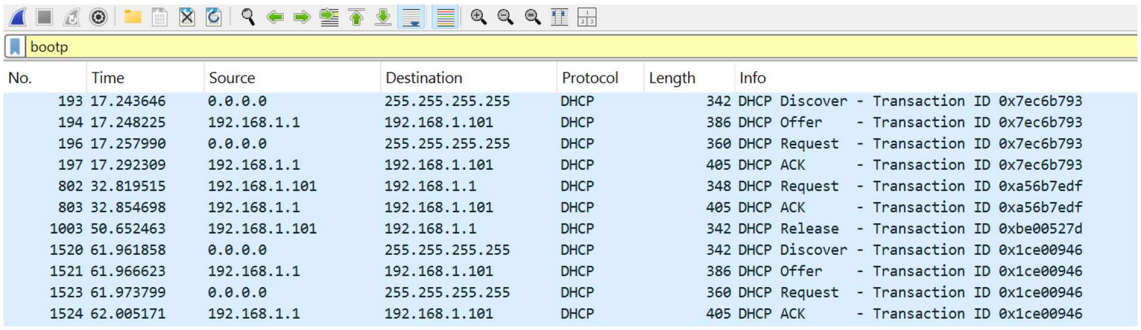
Part 2: Analyzing DHCP Traffic

Tổng quan

Phân tích chuyên sâu quá trình cấp phát địa chỉ IP tự động thông qua **Giao thức cấu hình Host động (DHCP)**, dựa trên dữ liệu gói tin đã được bắt giữ bằng Wireshark



bootp

No.	Time	Source	Destination	Protocol	Length	Info
193	17.243646	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0x7ec6b793
194	17.248225	192.168.1.1	192.168.1.101	DHCP	386	DHCP Offer - Transaction ID 0x7ec6b793
196	17.257990	0.0.0.0	255.255.255.255	DHCP	360	DHCP Request - Transaction ID 0x7ec6b793
197	17.292309	192.168.1.1	192.168.1.101	DHCP	405	DHCP ACK - Transaction ID 0x7ec6b793
802	32.819515	192.168.1.101	192.168.1.1	DHCP	348	DHCP Request - Transaction ID 0xa56b7edf
803	32.854698	192.168.1.1	192.168.1.101	DHCP	405	DHCP ACK - Transaction ID 0xa56b7edf
1003	50.652463	192.168.1.101	192.168.1.1	DHCP	342	DHCP Release - Transaction ID 0xbe00527d
1520	61.961858	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0x1ce00946
1521	61.966623	192.168.1.1	192.168.1.101	DHCP	386	DHCP Offer - Transaction ID 0x1ce00946
1523	61.973799	0.0.0.0	255.255.255.255	DHCP	360	DHCP Request - Transaction ID 0x1ce00946
1524	62.005171	192.168.1.1	192.168.1.101	DHCP	405	DHCP ACK - Transaction ID 0x1ce00946

1. Were any ARP packets sent or received during the DHCP packet-exchange period? If so, explain the purpose of those ARP packets.

No.	Time	Source	Destination	Protocol	Lengtl	Info
193	17.243646	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0x7ec6b793
194	17.248225	192.168.1.1	192.168.1.101	DHCP	386	DHCP Offer - Transaction ID 0x7ec6b793
196	17.257990	0.0.0.0	255.255.255.255	DHCP	360	DHCP Request - Transaction ID 0x7ec6b793
197	17.292309	192.168.1.1	192.168.1.101	DHCP	405	DHCP ACK - Transaction ID 0x7ec6b793
802	32.819515	192.168.1.101	192.168.1.1	DHCP	348	DHCP Request - Transaction ID 0xa56b7edf
803	32.854698	192.168.1.1	192.168.1.101	DHCP	405	DHCP ACK - Transaction ID 0xa56b7edf
1003	50.652463	192.168.1.101	192.168.1.1	DHCP	342	DHCP Release - Transaction ID 0xbe00527d
1520	61.961858	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0x1ce00946
1521	61.966623	192.168.1.1	192.168.1.101	DHCP	386	DHCP Offer - Transaction ID 0x1ce00946
1523	61.973799	0.0.0.0	255.255.255.255	DHCP	360	DHCP Request - Transaction ID 0x1ce00946
1524	62.005171	192.168.1.1	192.168.1.101	DHCP	405	DHCP ACK - Transaction ID 0x1ce00946

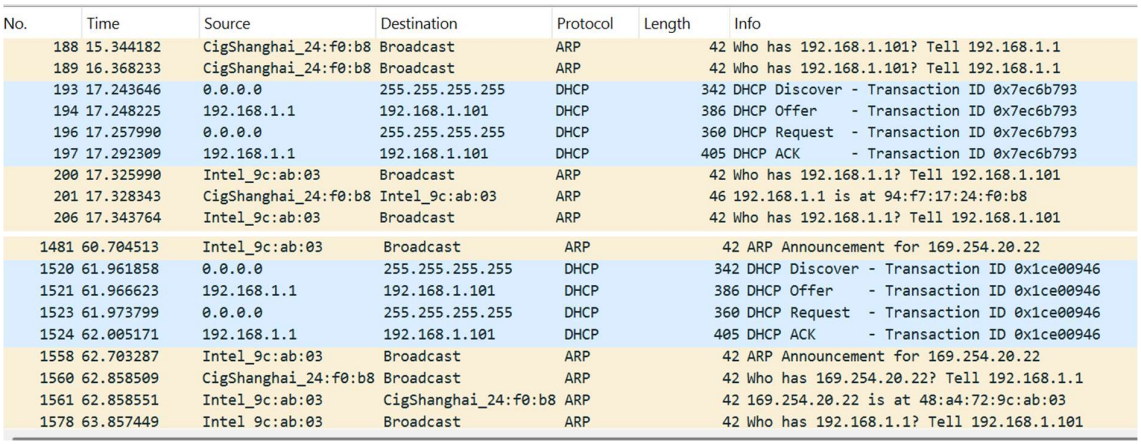
Dựa vào các dấu thời gian (Time) trong hình, ta có thể tính khoảng thời gian cho hai chu kỳ DORA hoàn chỉnh:

+ Chu kỳ thứ nhất (Transaction ID 0x7ec6b793)

- Bắt đầu (Discover): Gói tin 193 tại thời điểm 17.243646 giây.
- Kết thúc (ACK): Gói tin 197 tại thời điểm 17.292309 giây.
- Thời gian hoàn tất: 17.292309 - 17.243646 = 0.048663 giây.

+ Chu kỳ thứ hai (Transaction ID 0x1ce00946)

- Bắt đầu (Discover): Gói tin 1520 tại thời điểm 61.961858 giây.
- Kết thúc (ACK): Gói tin 1524 tại thời điểm 62.005171 giây.
- Thời gian hoàn tất: 62.005171 - 61.961858 = 0.043313 giây.



No.	Time	Source	Destination	Protocol	Length	Info
188	15.344182	CigShanghai_24:f0:b8	Broadcast	ARP	42	Who has 192.168.1.101? Tell 192.168.1.1
189	16.368233	CigShanghai_24:f0:b8	Broadcast	ARP	42	Who has 192.168.1.101? Tell 192.168.1.1
193	17.243646	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0x7ec6b793
194	17.248225	192.168.1.1	192.168.1.101	DHCP	386	DHCP Offer - Transaction ID 0x7ec6b793
196	17.257990	0.0.0.0	255.255.255.255	DHCP	360	DHCP Request - Transaction ID 0x7ec6b793
197	17.292309	192.168.1.1	192.168.1.101	DHCP	405	DHCP ACK - Transaction ID 0x7ec6b793
200	17.325990	Intel_9c:ab:03	Broadcast	ARP	42	Who has 192.168.1.1? Tell 192.168.1.101
201	17.328343	CigShanghai_24:f0:b8	Intel_9c:ab:03	ARP	46	192.168.1.1 is at 94:f7:17:24:f0:b8
206	17.343764	Intel_9c:ab:03	Broadcast	ARP	42	Who has 192.168.1.1? Tell 192.168.1.101
1481	60.704513	Intel_9c:ab:03	Broadcast	ARP	42	ARP Announcement for 169.254.20.22
1520	61.961858	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0x1ce00946
1521	61.966623	192.168.1.1	192.168.1.101	DHCP	386	DHCP Offer - Transaction ID 0x1ce00946
1523	61.973799	0.0.0.0	255.255.255.255	DHCP	360	DHCP Request - Transaction ID 0x1ce00946
1524	62.005171	192.168.1.1	192.168.1.101	DHCP	405	DHCP ACK - Transaction ID 0x1ce00946
1558	62.703287	Intel_9c:ab:03	Broadcast	ARP	42	ARP Announcement for 169.254.20.22
1560	62.858509	CigShanghai_24:f0:b8	Broadcast	ARP	42	Who has 169.254.20.22? Tell 192.168.1.1
1561	62.858551	Intel_9c:ab:03	CigShanghai_24:f0:b8	ARP	42	169.254.20.22 is at 48:a4:72:9c:ab:03
1578	63.857449	Intel_9c:ab:03	Broadcast	ARP	42	Who has 192.168.1.1? Tell 192.168.1.101

- Trong khoảng thời gian của 2 chu kì trên, không có gói tin ARP được trao đổi trong quá trình DHCP
- Giải thích nguyên nhân:

+ Sự vắng mặt của ARP trong quá trình DORA là do vai trò và cấp độ hoạt động khác nhau của hai giao thức:

- DHCP (DORA) hoạt động chủ yếu ở lớp Ứng dụng (Application Layer) và phục vụ mục đích cấp phát địa chỉ IP
- ARP hoạt động ở lớp Liên kết dữ liệu (Data Link Layer) và chỉ phục vụ mục đích phân giải địa chỉ MAC từ một địa chỉ IP đã biết

+ Mặc dù ARP không xuất hiện trong DORA, các gói ARP được ghi nhận xuất hiện ngay sau gói DHCP ACK là rất quan trọng và phục vụ 3 mục đích kỹ thuật chính:

- Phân giải địa chỉ MAC của Gateway: Sau khi máy nhận được địa chỉ IP và biết địa chỉ IP của Default Gateway qua DHCP ACK, nó phải sử dụng ARP để tìm địa chỉ MAC tương ứng của Gateway. Đây là bước bắt buộc để máy khách có thể đóng gói dữ liệu và gửi lưu lượng truy cập ra khỏi mạng cục bộ. Các gói ARP liên quan: ARP Request (*Who has 192.168.1.1? Tell 192.168.1.101*) và ARP Reply (ví dụ: Gói 200, 201,…).
- Kiểm tra xung đột IP (ARP Probe): Đây là một cơ chế phòng ngừa. Máy gửi một ARP Probe cho chính địa chỉ IP vừa được cấp phát. Nếu nhận được bất kỳ phản hồi nào, nó sẽ biết có sự xung đột địa chỉ IP (IP Conflict) và sẽ từ bỏ IP đó để bắt đầu lại quá trình DHCP. Các gói ARP liên quan: ARP Request (ví dụ: *Who has 192.168.1.101?*).
- Định danh địa chỉ mới (ARP Announcement): Máy có thể chủ động thông báo cho các thiết bị khác trong mạng rằng địa chỉ MAC của nó hiện được gán cho IP 192.168.1.101. Điều này giúp các máy khác cập nhật nhanh chóng bảng

ARP của chúng và tránh sự chậm trễ khi giao tiếp lần đầu. Gói tin liên quan: ARP Announcement (*ARP Announcement for 192.168.1.101*)

+ Phân tích bổ sung: APIPA
Sự hiện diện của các gói ARP liên quan đến địa chỉ 169.254.20.22 ngay trước chu kỳ DHCP thứ hai cho thấy một sự kiện quan trọng:

- Máy đã thất bại trong việc lấy IP từ DHCP Server trong một lần thử trước đó.
- Máy đã chuyển sang chế độ APIPA (Automatic Private IP Addressing) và tự gán địa chỉ IP trong dải 169.254.x.x.
- Các gói ARP Probe và Announcement là bằng chứng cho việc máy đang kiểm tra tính duy nhất của địa chỉ APIPA tự gán này, trước khi bắt đầu lại quy trình DHCP thành công (chu kỳ 2).

2. A host uses DHCP to obtain an IP address, among other configuration parameters. However, the host's IP address is not finalized until the completion of the four-message DHCP exchange. If the IP address is not assigned until the final message, what IP address values are used in the IP datagrams that carry these messages? (*For each of the four DHCP messages (DHCP Discover, DHCP Offer, DHCP Request, and DHCP ACK), specify the source and destination IP addresses used in the encapsulating IP datagrams.*)

- Quá trình DHCP sử dụng mô hình trao đổi bốn bước được gọi là DORA (Discover, Offer, Request, ACK). Đặc điểm quan trọng là máy chưa có địa chỉ IP hợp lệ cho đến khi hoàn tất bước cuối cùng, do đó việc đóng gói các thông điệp DHCP trong IP datagram yêu cầu các giá trị địa chỉ đặc biệt.

- Bảng phân tích địa chỉ IP trong từng thông điệp:

Thông điệp DHCP	IP Nguồn (Source IP)	IP Đích (Destination IP)	Vai trò

Discover (D)	0.0.0.0	255.255.255.255	Máy chưa có IP, broadcast tìm kiếm server
Offer (O)	192.168.1.1 (Server)	192.168.1.101 (IP đề xuất)	Server đề xuất IP, gửi unicast đến IP được đề xuất
Request (R)	0.0.0.0	255.255.255.255	Máy khách vẫn chưa có IP, broadcast thông báo chấp nhận
ACK (A)	192.168.1.1 (Server)	192.168.1.101 (IP đã gán)	Server xác nhận, gửi unicast đến IP đã cấp phát

- Phân tích các địa chỉ IP được Host Client sử dụng trong các bước Discover và Request:

Địa chỉ	Mục đích sử dụng
IP Nguồn: 0.0.0.0	Báo hiệu rằng Host chưa có IP. Lệnh Discover và Request được gửi khi ngăn xếp IP (IP Stack) của Client chưa được khởi tạo đầy đủ. 0.0.0.0 là địa chỉ "phi cấu hình" (unspecified address) để Host có thể tạo và gửi gói tin ở Lớp Mạng mà không cần IP hợp lệ.

IP Đích: 255.255.255.255	Đảm bảo gói tin Broadcast đến được tất cả các thiết bị trong mạng, đặc biệt là DHCP Server (vốn là thiết bị chưa được biết đến). Điều này cần thiết trong cả Discover (tìm kiếm DHCP server chưa biết vị trí) và Request (thông báo cho Server được chọn và các Server khác).

- Sự khác biệt rõ ràng nhất nằm ở cách DHCP Server (192.168.1.1) phản hồi lại trong các bước Offer và ACK:

Gói tin	IP đích trong lý thuyết (Broadcast)	IP đích trong dữ liệu thực tế (Unicast)
Offer và ACK	255.255.255.255	192.168.1.101

Phân tích Sự Khác Biệt:

+ Hiệu quả (Efficiency): Server đã quyết định gửi Offer và ACK trực tiếp đến địa chỉ IP mà nó đề xuất/vừa gán (192.168.1.101) thay vì gửi Broadcast. Đây là một cơ chế tối ưu hóa để giảm lưu lượng Broadcast trên mạng.

+ Khẳng định MAC (Layer 2): Server có thể làm điều này vì nó đã biết địa chỉ MAC của Client (được gửi trong gói Discover). Mặc dù IP (192.168.1.101) chưa được Client xác nhận chính thức, Server vẫn có thể đóng gói dữ liệu và gửi đến địa chỉ MAC của Client, dựa vào thông tin của Lớp 2.

+ Tính tạm thời của IP: Việc sử dụng địa chỉ 192.168.1.101 ngay từ gói Offer nhấn mạnh rằng địa chỉ IP đó, mặc dù chưa được xác nhận, đã có giá trị logic và được sử dụng để định danh Host trong phần còn lại của quá trình giao dịch.

3. If, after receiving the ACK, the client sent an ARP probe for this new IP but received an ARP Reply from *another* device, what specific action is the client required to take according to the DHCP standard (RFC 2131)

- Phát hiện xung đột thông qua ARP Probe:

Sau khi Host Client nhận được gói DHCP ACK từ Server, nó xem địa chỉ IP mới được gán là địa chỉ hợp lệ. Tuy nhiên, trước khi chính thức sử dụng, Host cần thực hiện bước xác minh cuối cùng để tránh xung đột địa chỉ IP (IP Address Conflict) trên mạng cục bộ

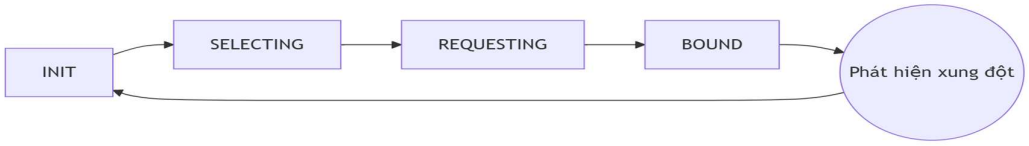
- Cơ chế: Host gửi một hoặc nhiều gói tin ARP Probe (ARP thăm dò) cho chính địa chỉ mới được cấp. Đây là các gói ARP không có địa chỉ IP nguồn để thăm dò
- Tình huống xung đột: Khi Host nhận được gói ARP Reply từ một thiết bị khác trên mạng, điều đó chứng tỏ địa chỉ IP đó đã được sử dụng

- Hành động bắt buộc theo Tiêu chuẩn RFC 2131:

- Gửi thông điệp DHCPDECLINE: Host Client phải ngay lập tức gửi một gói tin DHCPDECLINE đến DHCP Server.
- Mục đích của DHCPDECLINE: Thông báo cho DHCP server biết rằng địa chỉ IP được cấp phát không thể sử dụng do xung đột, yêu cầu server đánh dấu địa chỉ này là không khả dụng trong thời gian nhất định.

- Sau khi gửi DHCPDECLINE, Host Client không được phép sử dụng địa chỉ IP gây xung đột đó và phải chuyển sang trạng thái mới để xin cấp lại địa chỉ:

- Từ bỏ IP: Host phải lập tức hủy bỏ việc sử dụng địa chỉ IP xung đột đó.
- Chuyển trạng thái: Host chuyển về trạng thái INITIALIZING (Khởi tạo).
- Bắt đầu lại: Host sẽ khởi động lại toàn bộ quá trình xin cấp IP bằng cách gửi một gói DHCP Discover mới.



4. Why does the DHCP Request message still use UDP Port 68 as the source port and UDP Port 67 as the destination port, even though a unique, high-numbered ephemeral port could technically be used? Explain how

UDP's connectionless nature makes this fixed port usage simple and robust.

- Việc sử dụng các cổng cố định ((Port 68 và 67) trong DHCP, ngay cả trong thông điệp Request, là bắt buộc và phục vụ 2 mục đích chính:

+ Tiêu chuẩn hóa và nhận diện Ứng dụng

- Port đích (Destination Port 67): Đây là cổng được chỉ định cho DHCP Server. Mọi Host Client đều biết rằng để nói chuyện với DHCP Server, nó phải gửi gói tin đến Port 67.
- Port nguồn (Source Port 68): Đây là cổng được chỉ định cho DHCP Client. Việc sử dụng cổng cố định này là một phần của tiêu chuẩn DHCP, giúp Server nhận diện ngay lập tức rằng gói tin này đến từ một ứng dụng Client DHCP.

+ Hoạt động trong điều kiện chưa có IP:

- DHCP Request là một phần của quá trình DORA (thường xảy ra sau Discover/Offer). Trong bước Request, Host Client vẫn đang sử dụng Source IP là 0.0.0.0 (vì chưa có IP chính thức).
- Trong tình huống mà thông tin Lớp Mạng không đầy đủ (Source IP là 0.0.0.0 và Destination IP là Broadcast), việc sử dụng cổng cố định Port 68 là điều tối quan trọng. Nó đảm bảo rằng khi Server phản hồi lại bằng gói DHCP ACK, nó biết chính xác Port nào (Port 68) mà ứng dụng DHCP Client đang lắng nghe trên Host.

- Vai Trò Của Tính Chất Phi Kết Nối Của UDP:
UDP là giao thức phi kết nối (connectionless) và không trạng thái (stateless). Chính tính chất này giúp việc sử dụng các cổng cố định trở nên đơn giản và mạnh mẽ trong DHCP.

Đặc điểm của UDP	Ứng dụng trong DHCP	Lợi ích
Không bắt tay 3 bước	Client gửi Discover ngay lập tức (DHCP Discover) mà không cần thiết lập kết nối trước	Giảm overhead mạng, tăng tốc độ khởi động (bootstrap) cho Client

Không trạng thái (Stateless)	Mỗi message DHCP độc lập (Discover, Offer, Request, ACK)	Server không cần lưu trữ trạng thái kết nối (connection state) hoặc phiên làm việc (session state), giúp tăng khả năng mở rộng (scalability)
Không có sequence number	Không cần theo dõi thứ tự của các gói tin gửi/nhận	Đơn giản hóa việc triển khai (implementation) cả ở Client và Server; giảm thiểu xử lý ở tầng giao vận
Không có acknowledgment (ACK)	DHCP sử dụng Application-level ACK	Linh hoạt trong cơ chế thử lại (retry mechanism) và quản lý thời gian chờ (timeout) do bản thân DHCP tự xử lý logic độ tin cậy

5.

a. In the DHCP Discover packet, expand the User Datagram Protocol (UDP) layer and examine the Checksum field. Does Wireshark display the message "[UDP checksum is good]" or "[UDP checksum is incorrect]"?

- Trong gói tin DHCP Discover, khi mở rộng lớp User Datagram Protocol (UDP), trường Checksum hiển thị như sau:

- Giá trị Checksum: 0xd490
- Trạng thái: [unverified]

- CheckSum Status: Unverified

Kết luận: Wireshark không thể xác minh được tính toàn vẹn của Checksum, do đó không hiển thị trạng thái "good" hay "incorrect"

- Nguyên nhân kỹ thuật (Checksum Offloading):

+ Checksum Offloading là kỹ thuật tối ưu hóa hiệu suất, trong đó việc tính toán checksum được chuyển giao (offload) từ CPU sang phần cứng của card mạng (NIC).

+ Hậu quả khi Capture: Wireshark, chạy ở Lớp Liên kết dữ liệu (Data Link Layer) hoặc ngay trên Lớp Mạng (Network Layer) trong hệ điều hành, bắt giữ gói tin trước khi NIC kịp hoàn thành việc tính toán Checksum => giá trị Checksum mà Wireshark ghi lại có thể là giá trị tạm thời, không chính xác, hoặc chỉ là giá trị unverified (0xd490), khiến Wireshark không thể xác minh tính toàn vẹn của dữ liệu trong quá trình phân tích.

b. If the checksum had been calculated as incorrect, what action would the recipient's Transport Layer (UDP handler) have immediately taken, and why would this lead the DHCP process to stall?

- Nếu Checksum của gói tin DHCP Discover được tính toán là không chính xác (incorrect), Lớp Giao vận (UDP handler) của bên nhận sẽ ngay lập tức hủy gói tin, UDP handler sẽ loại bỏ (drop) gói tin đó tại lớp Transport và không chuyển tiếp nội dung (dữ liệu DHCP) lên Lớp Ứng dụng (DHCP Server). Lý do:

+ Tính toàn vẹn dữ liệu: Checksum được sử dụng để kiểm tra tính toàn vẹn (integrity) của dữ liệu. Nếu Checksum bị sai, điều đó có nghĩa là dữ liệu bên trong gói tin đã bị thay đổi, hỏng hóc, hoặc bị cắt xén trong quá trình truyền tải.

+ Không có cơ chế sửa lỗi: UDP là giao thức phi kết nối (connectionless) và không đáng tin cậy (unreliable). Không giống như TCP, UDP không có cơ chế sửa lỗi, không có khả năng yêu cầu gửi lại gói tin, hay thông báo lỗi cho bên gửi. Do đó, hành động duy nhất và bắt buộc là loại bỏ gói tin bị lỗi để tránh chuyển giao dữ liệu hỏng.

- Lý do quá trình DHCP bị đình trệ (stall):
+ Gói Discover không đến được Server: Gói DHCP Discover bị loại bỏ ở Lớp Giao vận (Transport Layer) của Server, nghĩa là DHCP Server (ứng dụng chạy ở Lớp Ứng dụng) không bao giờ nhận được yêu cầu cấp IP từ Client.

+ Không có phản hồi Offer: Nếu Server không nhận được gói Discover, nó sẽ không thể tạo và gửi gói DHCP Offer cho Client.

+ Hết thời gian chờ (Timeout) của Client: Host Client sẽ tiếp tục chờ gói DHCP Offer. Khi hết thời gian chờ, Client sẽ tự động gửi lại gói DHCP Discover. Nếu gói này tiếp tục bị lỗi Checksum, quá trình sẽ lặp lại cho đến khi Client từ bỏ và chuyển sang sử dụng địa chỉ APIPA (169.254.x.x), và chỉ có thể giao tiếp với thiết bị khác có APIPA trong cùng subnet

References

Computer Networking: A Top-Down Approach, 7th ed, Ross, J. K. (2005-2016). Wireshark Lab: DHCP v7.0.