DHCP server được sử dụng để phát hành các địa chỉ IP duy nhất và tự động định cấu hình các thông tin mạng khác. Trong hầu hết các gia đình và các doanh nghiệp nhỏ, router hoạt động như DHCP server. Trong các mạng lớn, một máy tính duy nhất có thể hoạt động như một DHCP server.

Nói tóm lại, quá trình này diễn ra như sau: Một thiết bị (client) yêu cầu một địa chỉ IP từ một router (máy chủ), sau đó host sẽ gán một địa chỉ IP có sẵn để cho phép client giao tiếp với mạng.

Khi một thiết bị đã được bật và kết nối với mạng có DHCP server, nó sẽ gửi một yêu cầu đến máy chủ này, được gọi là yêu cầu DHCPDISCOVER. Sau khi gói tin DISCOVER đến DHCP server, máy chủ sẽ cố gắng giữ một địa chỉ IP mà thiết bị có thể sử dụng, và sau đó cung cấp cho client địa chỉ này với một gói DHCPOFFER.

Sau khi cung cấp địa chỉ IP đã chọn, thiết bị đáp ứng với DHCP server bằng một gói tin DHCPREQUEST để chấp nhận nó, sau đó máy chủ gửi ACK được sử dụng để xác nhận thiết bị có địa chỉ IP cụ thể đó và để xác định khoảng thời gian mà thiết bị có thể sử dụng địa chỉ trước khi lấy địa chỉ mới. Nếu máy chủ quyết định rằng thiết bị không có địa chỉ IP, nó sẽ gửi một NACK. Tất nhiên điều này xảy ra rất nhanh và bạn không cần biết bất kỳ loại kỹ thuật nào được sử dụng để lấy địa chỉ IP từ DHCP server.

**Các thành phần của DHCP**

Khi làm việc với DHCP, bạn cần hiểu tất cả thành phần của nó. Dưới đây là danh sách các thành phần của DHCP.

* **DHCP server:** Một thiết bị mạng chạy dịch vụ DHCP chứa địa chỉ IP và thông tin cấu hình liên quan. Đây thường là máy chủ hoặc [router](https://quantrimang.com/kien-thuc-co-ban-ve-mang-phan-2-router-35172) nhưng có thể là bất cứ thứ gì hoạt động như máy chủ chẳng hạn như thiết bị SD-WAN.
* **DHCP client**: Thiết bị nhận thông tin cấu hình từ máy chủ DHCP. Đây có thể máy tính, thiết bị di động, thiết bị IoT ([Internet of Things](https://quantrimang.com/internet-of-things-iot-hay-mang-luoi-van-vat-ket-noi-la-gi-131856)) hoặc bất cứ thiết bị gì khác yêu cầu kết nối mạng. Hầu hết các thiết bị này được cấu hình để nhận thông tin DHCP theo mặc định.
* **IP address pool**: Dãy địa chỉ có sẵn cho client DHCP. Những địa chỉ này thường được truyền tuần tự từ thấp nhất đến cao nhất.
* **Subnet**: Mạng IP có thể được phân thành các phân đoạn được gọi là subnet (mạng con). [Mạng con](https://quantrimang.com/internet-that-la-don-gian-phan-chia-mang-thanh-cac-mang-con-798) giúp mạng được quản lý dễ dàng hơn.
* **Lease**: Khoảng thời gian client DHCP giữ thông tin địa chỉ IP. Khi khoảng thời gian này hết hạn, client phải làm mới nó.
* **DHCP relay**: Router hoặc máy chủ nghe tin nhắn được phát trên mạng đó và sau đó chuyển chúng đến một máy chủ được cấu hình. Máy chủ này sau đó phản hồi lại relay agent để truyền chúng đến client. Nó được sử dụng để tập trung máy chủ DHCP thay vì để máy chủ trên mỗi mạng con.

Design Goals

Cơ chế chứ không phải là một chính sách.

client không yêu cầu cấu hình lại thủ công.

Nó không nên yêu cầu một máy chủ trên mạng con.

Nó phải tương tác với các đại lý chuyển tiếp BOOT và cung cấp dịch vụ cho các khách hàng của BOOTP.

DHCP must

Đảm bảo địa chỉ mạng duy nhất.

Giữ lại cấu hình máy khách DHCP trong quá trình khởi động lại máy khách.

Cho phép tự động gán các tham số cấu hình cho khách hàng mới.

Hỗ trợ phân bổ cố định các tham số cấu hình cho các khách hàng cụ thể.

DHCP Messages

DHCPDECLINE - Máy khách đến máy chủ cho biết địa chỉ mạng đã được sử dụng.

DHCPRELEASE - Máy khách đến máy chủ từ bỏ địa chỉ mạng và hủy hợp đồng thuê còn lại.

DHCPINFORM - Máy khách đến máy chủ, chỉ yêu cầu các tham số cấu hình cục bộ; khách hàng đã có địa chỉ mạng được cấu hình bên ngoài.

State transition diagram Sơ đồ chuyển trạng thái

Reacquisition and expiration Tái chế và hết hạn

Lần T1 và T2 để gia hạn hợp đồng thuê

Tại T1, khách hàng vào trạng thái KHAI THÁC

Tại T2, khách hàng chuyển sang trạng thái REBINDING

T1 <T2 <thời gian hết hạn thuê

Ở một trong hai trạng thái, máy khách gửi DHCPREQUEST

Nếu hết hạn thuê trước DHCPACK, máy khách sẽ chuyển sang trạng thái INIT

Enhancements Cải tiến

Tích hợp DHCP với DNS

Phân bổ địa chỉ Multicast

Phát hiện máy chủ DHCP trái phép

Phân cụm cho tính sẵn sàng cao

Performance Issues

Thời hạn thuê phù hợp

Kéo dài thời gian thuê cho các mạng lớn, cố định

Rút ngắn thời gian thuê cho các mạng biến đổi có ít địa chỉ IP hơn

Địa chỉ dự trữ có đặt phòng

Tích hợp DHCP với các dịch vụ khác

2.

DHCP-Snooping là tính năng chống giả mạo DHCP Server, chỉ những DHCP Server được sự cho phép của Admin mới có quyền cấp DHCP cho máy tính trong mạng.  
Tính năng chống giả mạo IP hay chống giả mạo MAC Address (ARP Inspection) đều hoạt động dựa trên DHCP-Snooping. Chính vì vậy DHCP-Snooping là công cụ không thể thiếu khi muốn nâng cao tính bảo mật cho mạng LAN bằng cách ngăn chặn những người dùng sử dụng phần mềm giả mạo MAC, IP với mục đích xấu.

Khi DHCP snooping được kích hoạt, cổng trên Switch sẽ phân loại thành cổng tin cậy (trusted) và không tin cậy (untrusted). Cổng tin cậy cho phép nhận DHCP Reply hay cổng được kết nối với Server DHCP. Nếu DHCP Server giả mạo gắn vào cổng “untrusted” và gởi DHCP Reply thì gói Reply sẽ bị loại bỏ. Các cổng nào bị vi phạm sẽ tự động shutdown chuyển sang trang thái err-disable.

**Tại sao chúng ta cần DHCP Snooping?**  
  
Chúng ta cần DHCP Snooping để ngăn chặn các cuộc tấn công “man-in-the-middle”. Giả sử tồn tại một kẻ tấn công “man-in-the-middle” giả mạo DHCP server và trả lời cho gói tin DHCPDISCOVER trước khi DHCP Server thực trả lời, từ đó DHCP giả mạo sẽ gửi thông tin cấu hìn IP trong đó có gateway giả mạo. Khi máy tính của người dùng gởi dữ liệu đến gateway để ra mạng bên ngoài, máy tính của kẻ tấn công sẽ trở thành gateway trong trường hợp này. Kẻ tấn công có thể phân tích nội dung của mỗi gói dữ liệu được gởi đến trước khi thực hiện chuyển tiếp thông thường.

Trusted and Untrusted Sources

Máy chủ đáng tin cậy: các thiết bị dưới sự kiểm soát của quản trị viên là các nguồn đáng tin cậy bao gồm các bộ chuyển mạch, bộ định tuyến và máy chủ trong mạng của bạn.

Máy chủ không đáng tin cậy: Máy chủ DHCP trên mạng của bạn mà bạn không biết về cổng không tin cậy được gọi là máy chủ DHCP tải giả.

Dhcp snooping feature

Kích hoạt DHCP snooping trên cổng Không tin cậy

Lọc các tin nhắn không hợp lệ

Lưu lượng giới hạn lưu lượng đáng tin cậy và không đáng tin cậy

Duy trì cơ sở dữ liệu ràng buộc DHCP snooping

Theo mặc định, nó không hoạt động trên tất cả các Vlan

Notification of DHCP Snooping

DHCP snooping cho phép cấu hình cổng là đáng tin cậy và không đáng tin cậy

Các cổng không tin cậy không thể xử lý trả lời DHCP

Cấu hình DHCP snooping trên cổng uplink đến máy chủ DHCP.

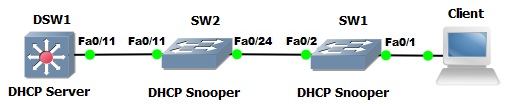
Don Cấu hình DHCP snooping trên các cổng máy khách

Ingress Source Filtering

Ngoài việc lọc các tin nhắn DHCP không đáng tin cậy, DHCP Snooping có thể cho phép người dùng định cấu hình Lọc nguồn Ingress như một tính năng bảo mật. Khi Bộ lọc nguồn Ingress (ISF) được bật trên một cổng hoặc cổng linkagg, các gói ban đầu được phép cho lưu lượng truy cập là DHCP, DNS và ARP để cho phép máy khách lấy và địa chỉ IP từ máy chủ DHCP trong đó Liên kết MAC-IP mục nhập được tạo trong tác vụ DHCP Snooping, sau đó nó sẽ cho phép các gói khớp với kết hợp địa chỉ IP / địa chỉ MAC / cổng được lấy từ mục nhập bảng liên kết snooping của DHCP. Các gói không phù hợp khác sẽ bị loại bỏ.

SW1(config)#ip dhcp snooping  
  
Chúng ta cần phải kích hoạt cho các VLAN, trong trường hợp này chúng ta chỉ dùng cho VLAN1  
SW1(config)#ip dhcp snooping vlan 1  
  
Bây giờ chúng ta sẽ cấu hình interface f0/1 kết nối với DSW1 là một trusted port:  
SW1(config)#interface f0/1  
SW1(config-if)#ip dhcp snooping trust  
  
Chúng ta nên kích hoạt rate limiting trên các cổng untrusted để giới hạn packet được truyền nhận mỗi giây. Được sử dụng để ngăn chặn việc tấn công DHCP server bằng cách gửi rất nhiều yêu cầu đến DHCP server làm cho DHCP server cạn kiệt các IP cung cấp cho client  
SW1(config)#interface f0/1  
SW1(config-if)#ip dhcp snooping limit rate 25  
  
**Kiểm tra**  
Bây giờ chúng ta sẽ kiểm tra lại cấu hình DHCP Snooping  
SW1#show ip dhcp snooping  
Switch DHCP snooping is enabled  
DHCP snooping is configured on following VLANs: 1  
Insertion of option 82 is enabled  
Option 82 on untrusted port is not allowed  
Verification of hwaddr field is enabled  
Interface Trusted Rate limit (pps)  
----------------------- ------- ----------------  
FastEthernet0/24 no unlimited   
FastEthernet0/1 yes 25  
  
Tiếp theo chúng ta sẽ kết nối máy tính client vào cổng Fa0/24 trên SW1 để xin IP động, chúng ta có thể thấy các IP được cấp đã được DHCP Snooping lưu lại:  
SW1#show ip dhcp snooping binding   
MacAddress IpAddress Lease(sec) Type VLAN Interface

**DHCP Option 82**

Do khi kích hoạt tính năng DHCP Snooping trên SW1, DHCP Option 82 sẽ được thêm vào các DHCP packet khi đi qua một switch. Option 82 chứa thông tin cụ thể về port mà client kết nối tới. Các gói tin DHCP cũng mang theo một trường “giaddr” mặc định được thiết lập là 0.0.0.0 (một giá trị khác 0)   
Khi DHCP Snooping hoặc DHCP relay agent được kích hoạt, DHCP Option 82 sẽ được thêm vào DHCP packet khi đi qua một switch. Option 82 chứa thông tin cụ thể về port mà client kết nối tới.  
[](http://www.vnpro.vn/khai-giang/)  
Hình 3. Mô hình DHCP Snooping Option 82  
  
Trong mô hình này, các cổng đối diện với DHCP Server là Fa0/2 trên SW1, Fa0/11 trên SW2, các cổng này đã được cấu hình là trusted. Mặc định SW1 sẽ chèn DHCP Option 82 vào tất cả các packet mà nó nhận được từ client. Cũng theo mặc định thì SW2 sẽ hủy các packet này khi nhận được vì một switch khi DHCP Snooping được kích hoạt sẽ hủy các packet trên cổng untrusted có chứa Option 82 hoặc có giaddr khác 0 (ví dụ 0.0.0.0). Dưới đây là thông điệp mà chúng ta nhìn thấy nếu debug trên SW2 khi SW1 gửi DHCPDISCOVER ra cổng Fa0/2  
%DHCP\_SNOOPING-5-DHCP\_SNOOPING\_NONZERO\_GIADDR: DHCP\_SNOOPING drop message with non-zero giaddr or option82 value on untrusted port  
Chúng ta có thể thấy cổng Fa0/24 trên SW2 là một cổng untrusted cho nên nó sẽ hủy các packet từ Client gửi đến vì có chứa Option 82 do trên SW1 đã kích hoạt DHCP Snooping, các packet sẽ không bao giờ đến được DSW1. Chúng ta sẽ giải quyết vấn đề này bằng cách sử dụng một lệnh trên SW2 sẽ trusted các gói tin chứa DHCP Option 82 được nhận trên cổng untrusted (Fa0/24).  
SW2(config)#ip dhcp snooping information option allow-untrusted  
Bởi vì DHCP Server của chúng ta là một thiết bị Cisco IOS, mặc định nó sẽ từ chối các gói tin chứa Option 82 nên chúng ta cũng cần phải trust trên DSW1  
DSW1(config)#ip dhcp relay information trust-all  
Ngoài ra chúng ta còn có một số cách khác như cấu hình trusted trên Fa0/24 của SW2 hoặc chúng ta có thể cấu hình trên SW1 (SW1(config)# #no ip dhcp snooping information option).