Lab: Sử dụng Postman tương tác với SD-WAN REST API

1. Mô tả

- Sử dụng công cụ Postman tạo Collection để chứa các request xác thực và lấy thông tin từ SD-WAN vManage
- Sử dụng công cụ Postman thực hiện gửi các request đến SD-WAN (vManage) để lấy thông tin thiết bị, template
- Từ Collection trong Postman, tiến hành tạo request để xác thực với vMange
- Sau khi xác thực thành công thì tiếp tục tạo các request để lấy thông tin những thiết bị có trong Controller

2. Yêu cầu kỹ thuật

- Cài đặt công cụ Postman (Bài lab sử dụng Postman version 9.15.11)
- Kết nối đến SD-WAN vManage, thông tin Vmanage trong bài lab:
  - ❖ Host: https://sandbox-sdwan-1.cisco.com
  - ❖ Username: devnetuser
  - ❖ Password: RG!_Yw919_83
- Tạo các requet để xác thực, lấy thông tin thiết bị có trong SD-WAN

3. Thực hiện

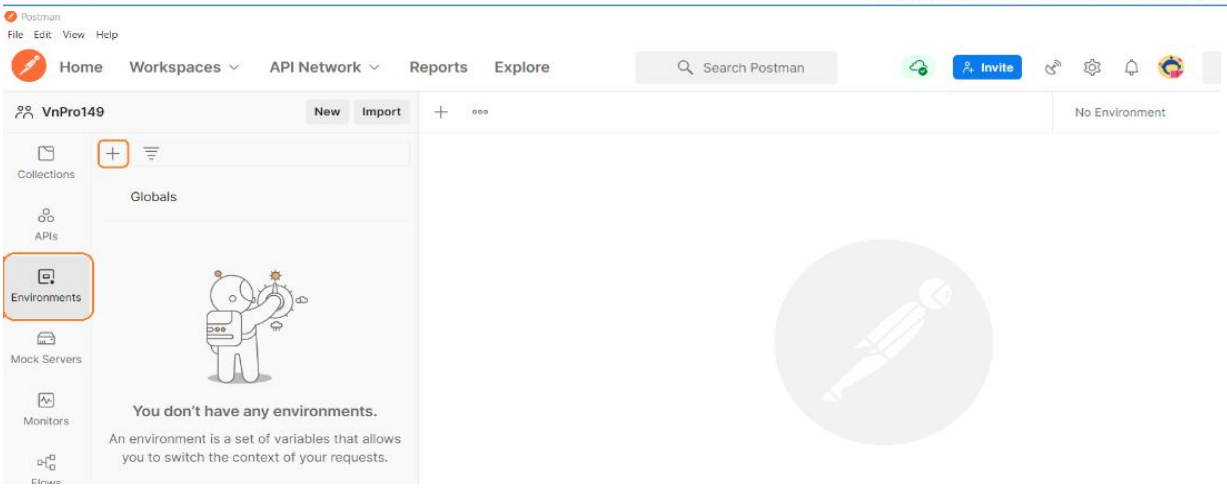
a. Tạo môi trường

Sử dụng Environment trong Postman như một nơi để lưu trữ "biến" để có thể tái sử dụng ở nhiều nơi.

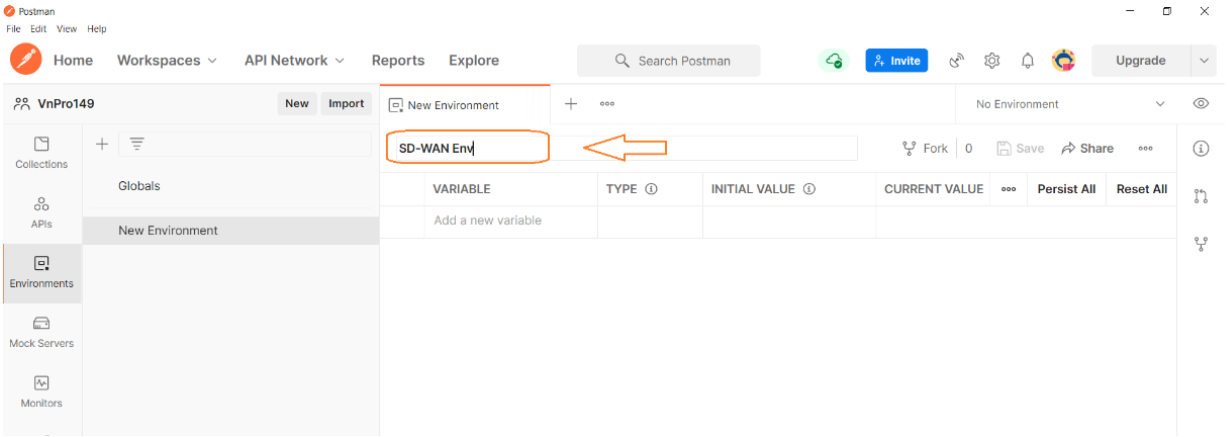
Ở Postman sẽ chia làm 2 loại Environments: Local và Global

- Local: Phạm vi ảnh hưởng chỉ có khi chọn đúng Enviroments.
- Global: Phạm vi ảnh hưởng đến toàn bộ các project có trong Postman, nhưng nếu có 2 biến cùng tên ở Local và Global thì sẽ ưu tiên lấy Local.

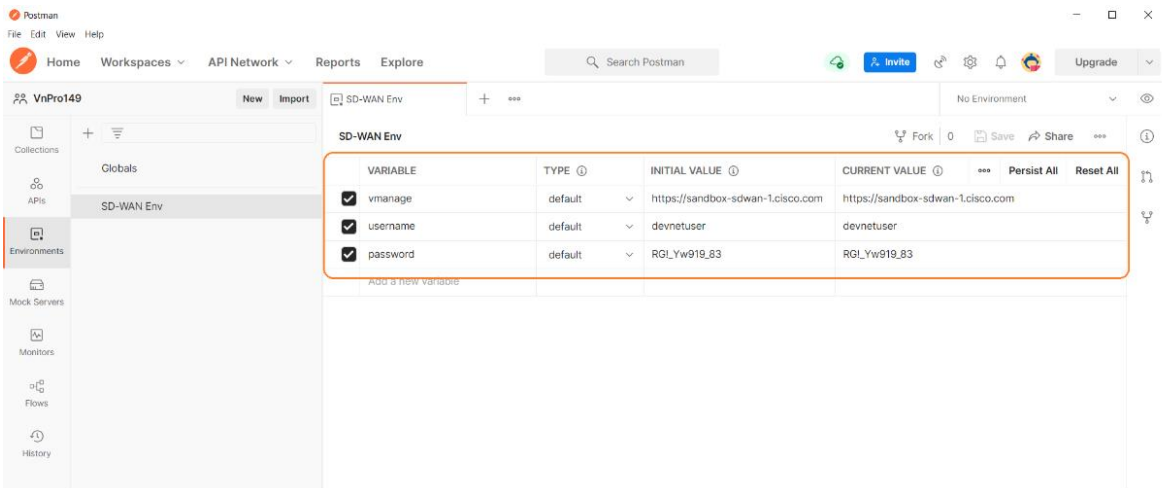
Bước 1: Để tạo môi trường, bạn cần vào phần Environment sau đó ấn vào dấu cộng phía góc trái



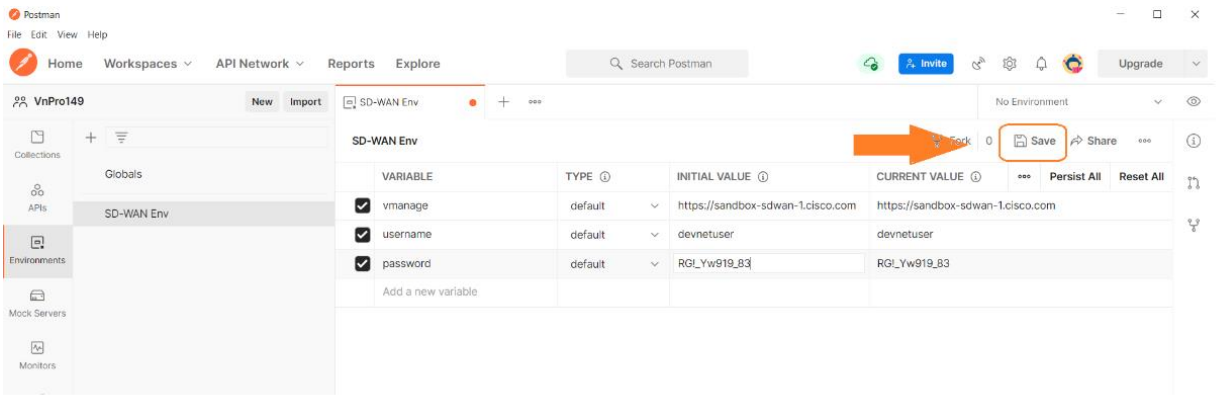
Bước 2: Nhập tên môi trường



Bước 3: Điền thông tin truy cập của vManage vào môi trường để có thể sử dụng nhiều nơi



Bước 4: Nhấn save để lưu

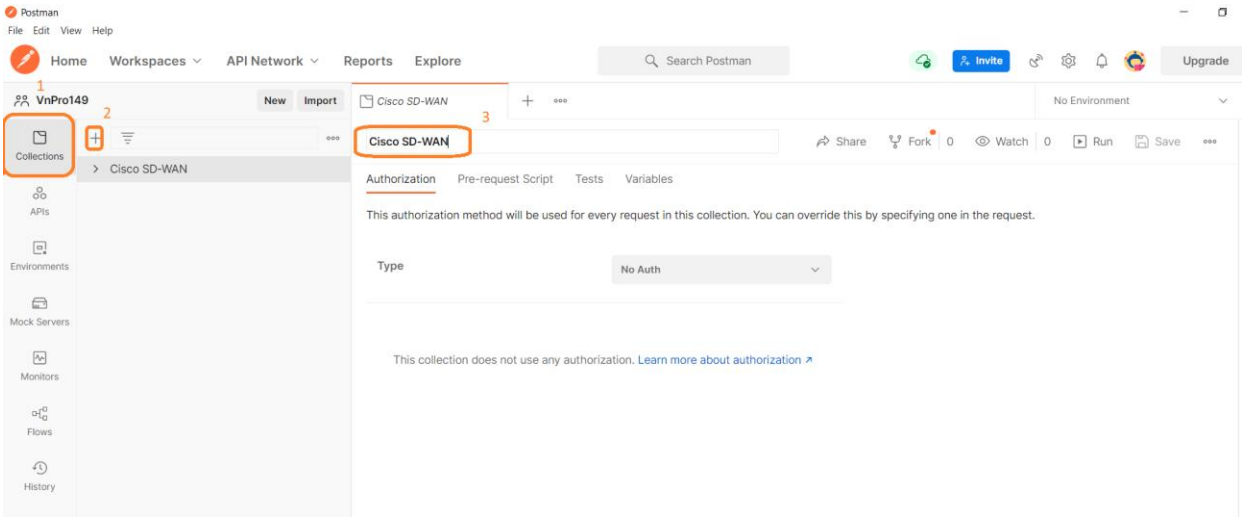


b. Xác thực

Thông thường việc đầu tiên khi chúng ta tương tác với API đó là việc xác thực. Xác thực để đảm bảo rằng chỉ những người dùng có quyền mới có thể truy cập vào API. Chúng ta có thể sử dụng các tính năng RBAC để có thể giới hạn quyền truy cập tài nguyên.

Để hiểu rõ hơn về các xác thực của **CISCO SD-WAN REST API**, bạn có thể tham khảo thêm tài liệu trên trang chính thức của Cisco: https://developer.cisco.com/sdwan/

Bước 1: Tạo collection

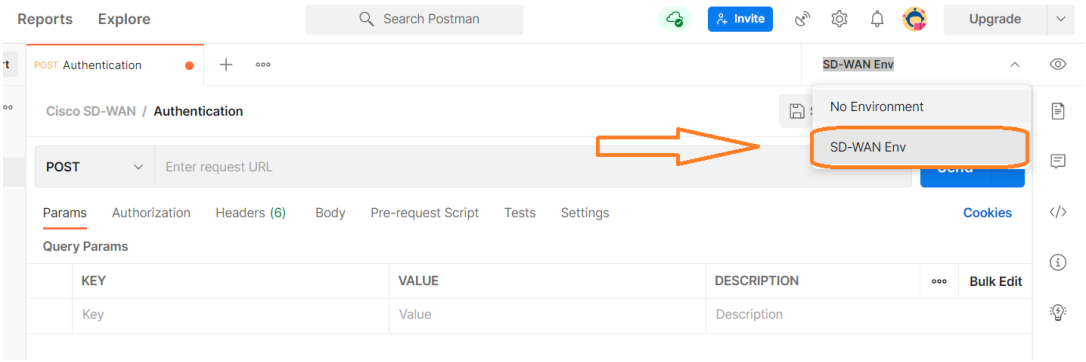


Bước 2: Tạo một request để xác thực

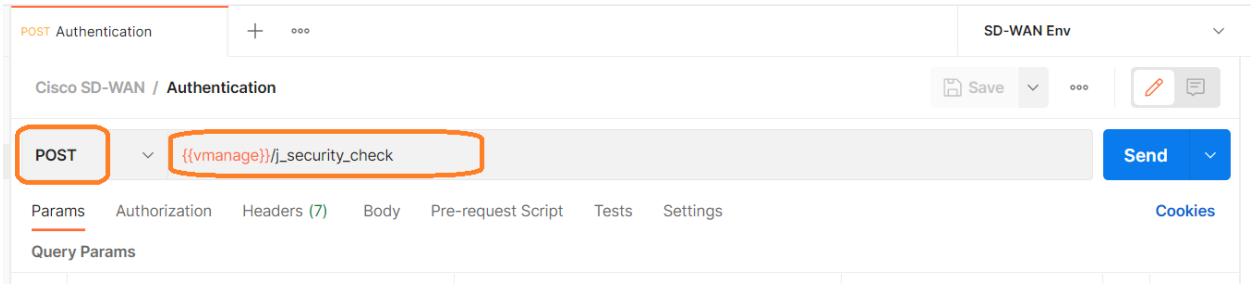
Bên trong Cisco-SD-WAN collection, tạo mội API request đặt tên là **Authentication**.

- Authentication call sử dụng phương thức POST
- Để xác định địa chỉ của vManage chúng ta sử dụng biến môi trường *{{vmanage}}* đã tạo ở phần trước. Biến môi trường sẽ được thay thế bằng giá trị đã tạo trong môi trường khi gửi request.
- Địa chỉ mà chúng ta trỏ đến là *j_check_security*

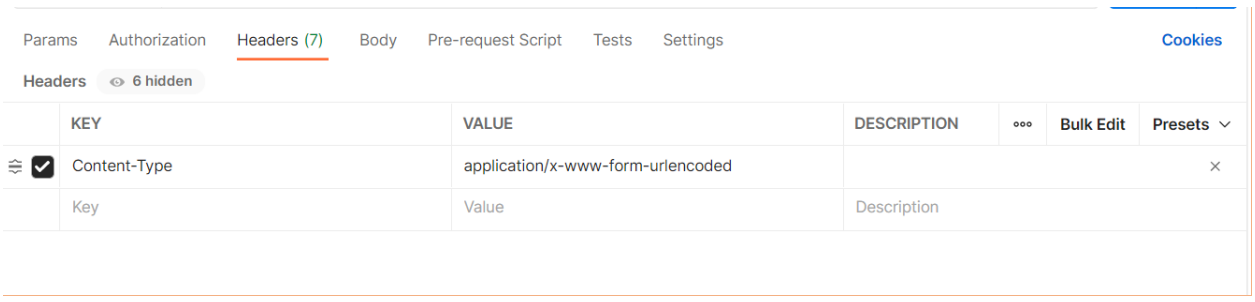
Chọn đúng môi trường đã tạo



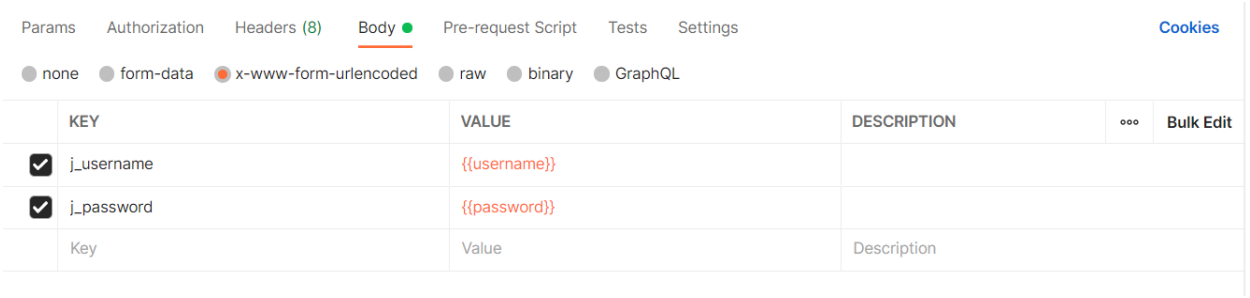
Điền request URL



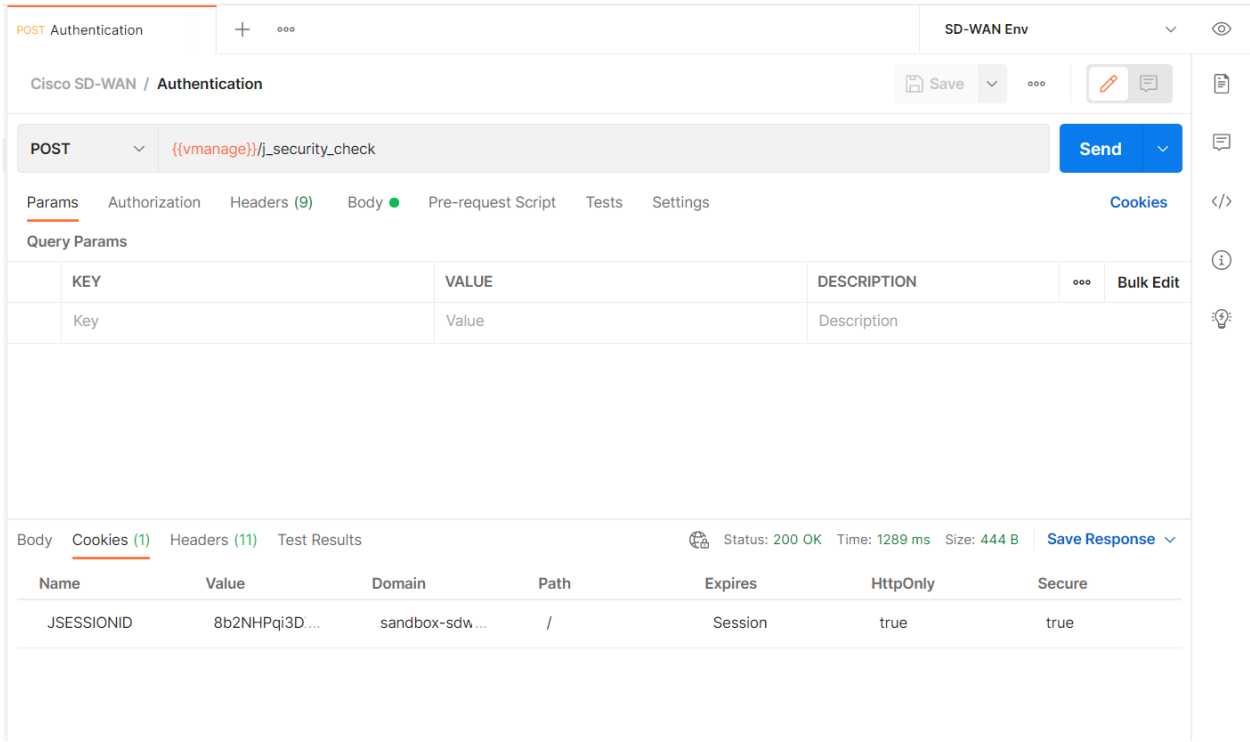
Dưới phần **Headers** tab, nhập thông tin Content-Type



Thông tin username và password được điền vào **Body** tab với key là j_username và j_password, phần value gọi lại biến trong môi trường

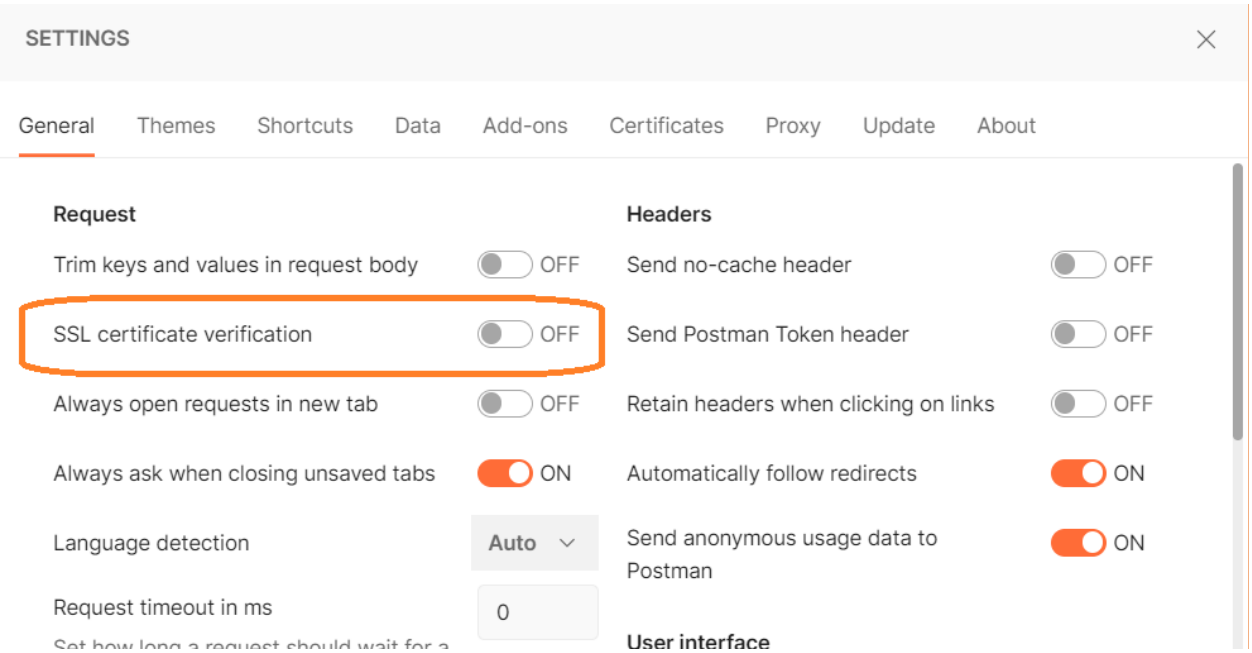


Sau khi đã điền tất cả những tham số cần thiết để xác thực với vManage: địa chỉ vManage, phương thức, header và body. Nhấn nút **Send** và trả về kết quả như sau:



Phần **Body** sẽ không trả về bất kỳ thông tin nào và status phải là 200 OK. Chú ý phần Cookie sẽ trả về JSESSIONID và giá trị bên trong. Thông tin **Cookie** đó sẽ được sử dụng để xác thực cho lần gọi API tiếp theo, cookie chỉ tồn tại trong một khoảng thời gian nhấy định.

Lưu ý: Nếu bạn sử dụng SD-WAN vManage của cá nhân và chưa được cấu hình SSL thì bạn phải vào phần File > Setting > tắt chức năng SSL certificate verification



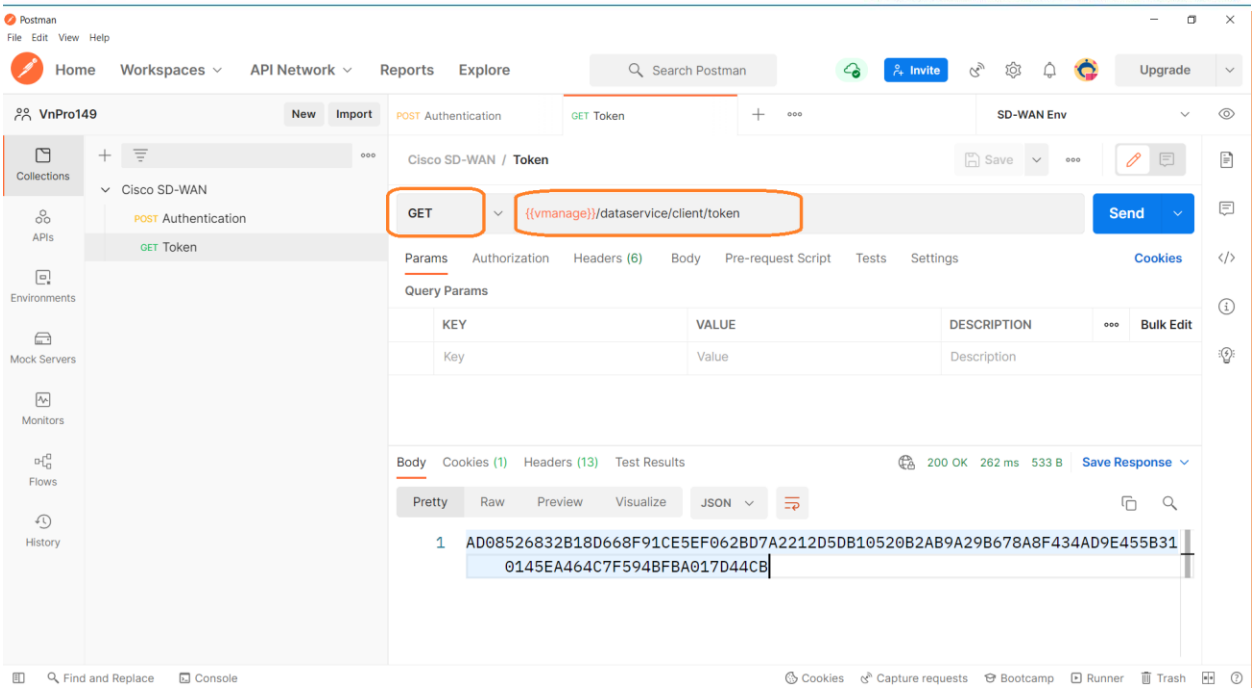
Bước 3: Phòng Ngừa API CSRF

CSRF hay còn gọi là kỹ thuật tấn công "**Cross-site Request Forgery**", nghĩa là kỹ thuật tấn công giả mạo chính chủ thể của nó. **CSRF** nói đến việc tấn công vào chứng thực request trên web thông qua việc sử dụng Cookies. Đây là nơi mà các hacker có khả năng sử dụng thủ thuật để tạo request mà bạn không hề biết.

Tính năng này được sử dụng để chống kỹ thuật tấn công giả mạo (CRSF) có thể xảy ra khi sử dụng Cisco SD-WAN REST APIs. Ở đây chúng ta sử dụng crsf_token để phòng chống CSRF, token này sẽ được đính kèm trong các lần gọi API và sẽ thay đổi liên tục trong phiên làm việc. Nếu token được sinh ra và token được gửi lên ko trùng nhau thì loại bỏ request.

Tạo một request mới để thực hiện lấy Token:

- Sử dụng phương thức Get
- Resource trỏ đến là /dataservice/client/token

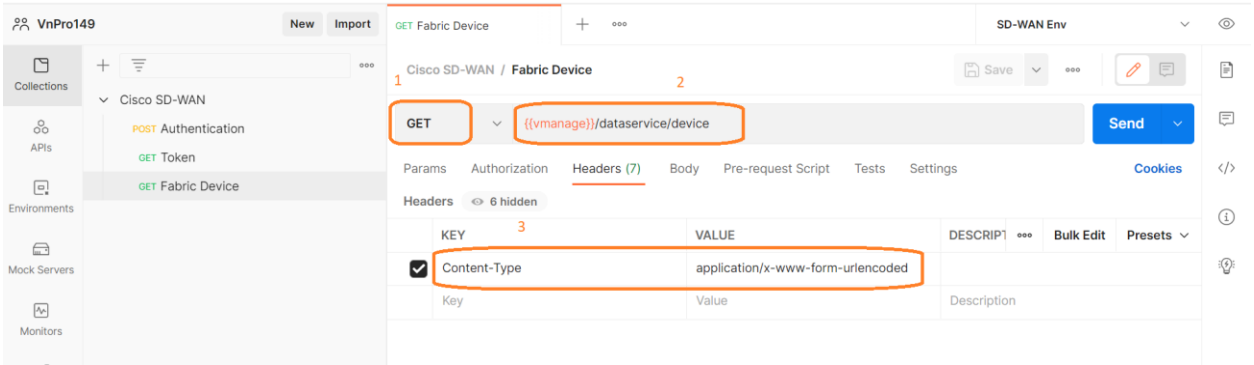


c. Lấy thông tin và trạng thái thiết bị SD-WAN

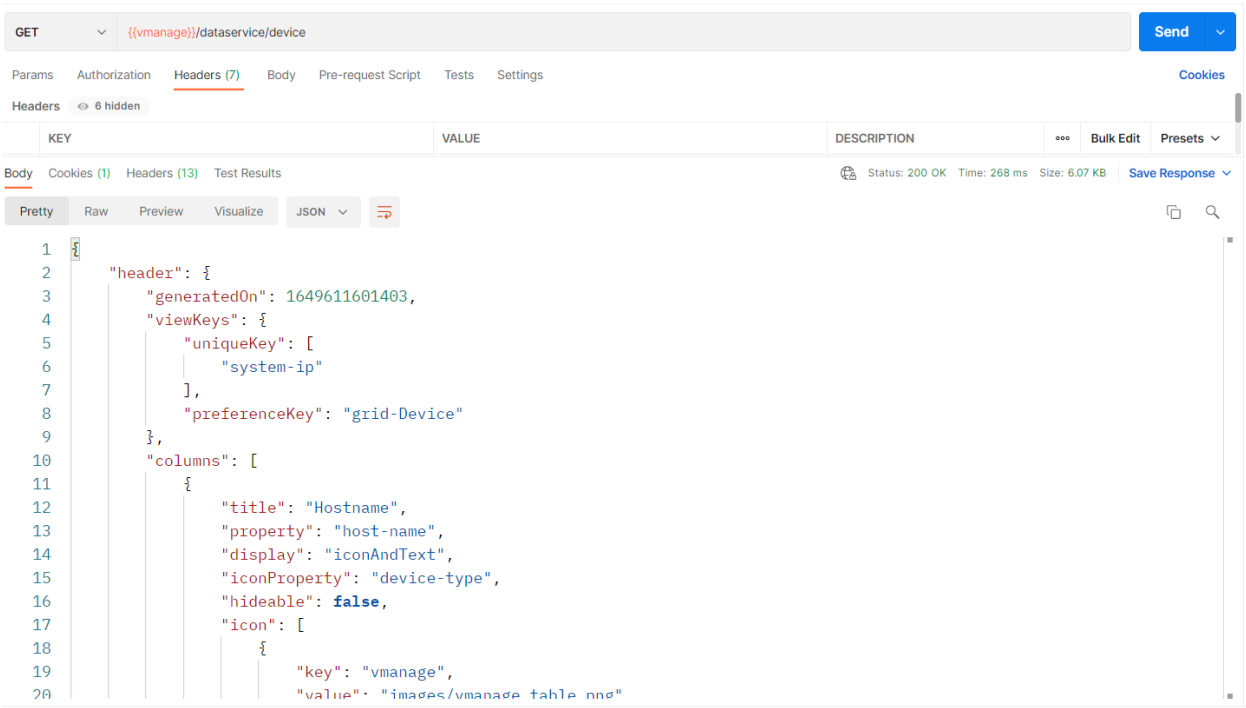
Sau khi đã xác thực thành công và có được JSESSIONID cookie, bây giờ bạn có thể truy xuất dữ liệu từ **Cisco SD-WAN REST API**.

Bước 1: Danh sách thiết bị

Để lấy được danh sách thiết bị chúng ta sử dụng phương thức GET cùng với resource đến api endpoint là /dataservice/device. Dữ liệu sẽ được trả về với định dạng JSON cùng với danh sách của tất cả thiết bị có trong SD-WAN fabric:



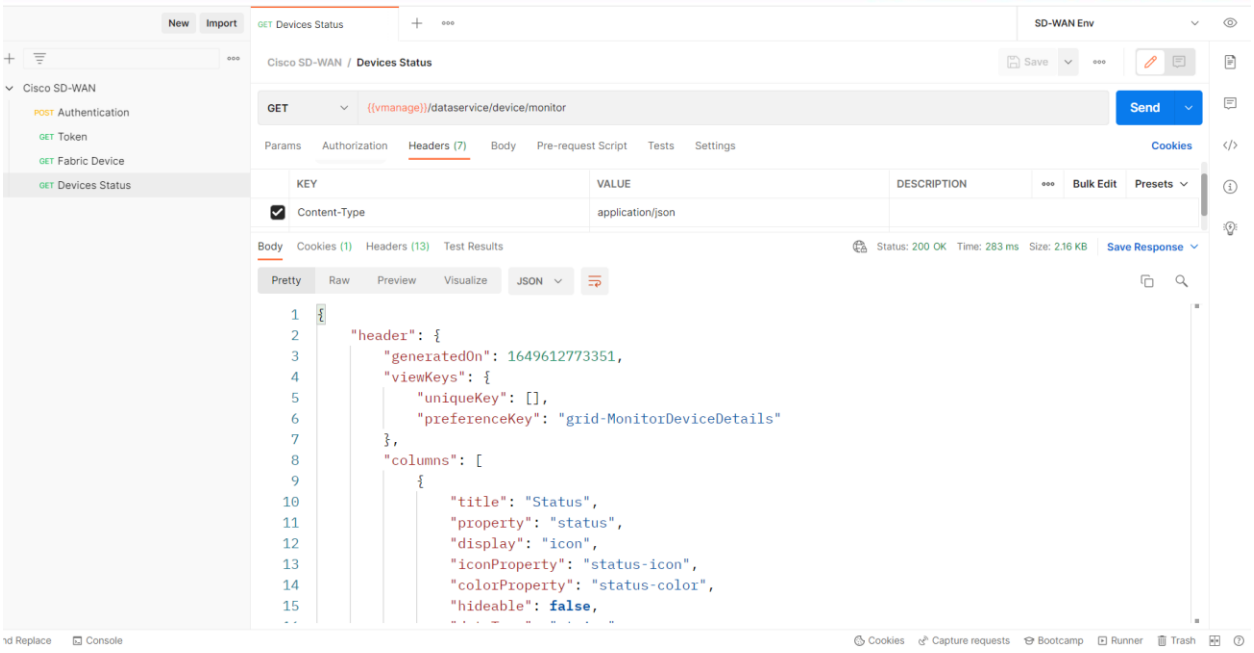
Sau khi nhấn **Send** sẽ trả về kết quả tương tự như hình:



Nếu bạn không nhận được kết quả như hình, kiểm tra lại status code đã trả về 200 OK. Nguyên nhân có thể do JSESSIONID cookie đã hết hạn, nếu vậy bạn cần phải xác thực lại.

Bước 2: Trạng thái thiết bị

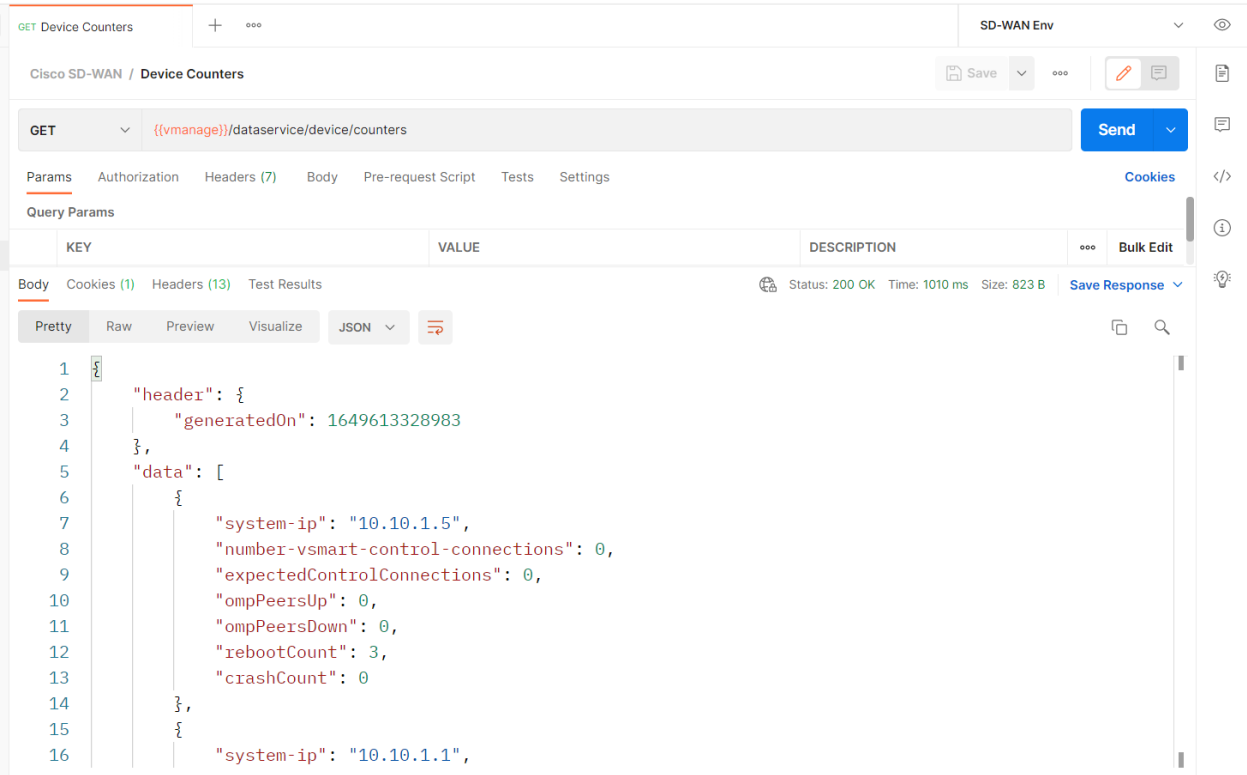
Request tiếp theo được tạo trong collection được gọi để xem thông tin cụ thể trạng thái của tất cả thiết bị trong fabric. Sử dụng phương thức GET và trỏ đến resource /data/device/monitor.



d. Lấy thông tin device counters và interface statistics

Nếu bạn muốn có thêm thông tin liên quan đến các kết nối của fabric, số lần thiết bị được khởi động lại và nhiều thông tin khác. Nếu bạn tìm kiếm trong **API Documentation**, bạn sẽ tìm thấy resource /dataservice/device/counters.

Kết quả trả về như sau:



Tiếp theo, lấy thông tin số liệu thống kê của các interface có trong SD-WAN fabric sử dụng resource /dataservice/statistics/interface.