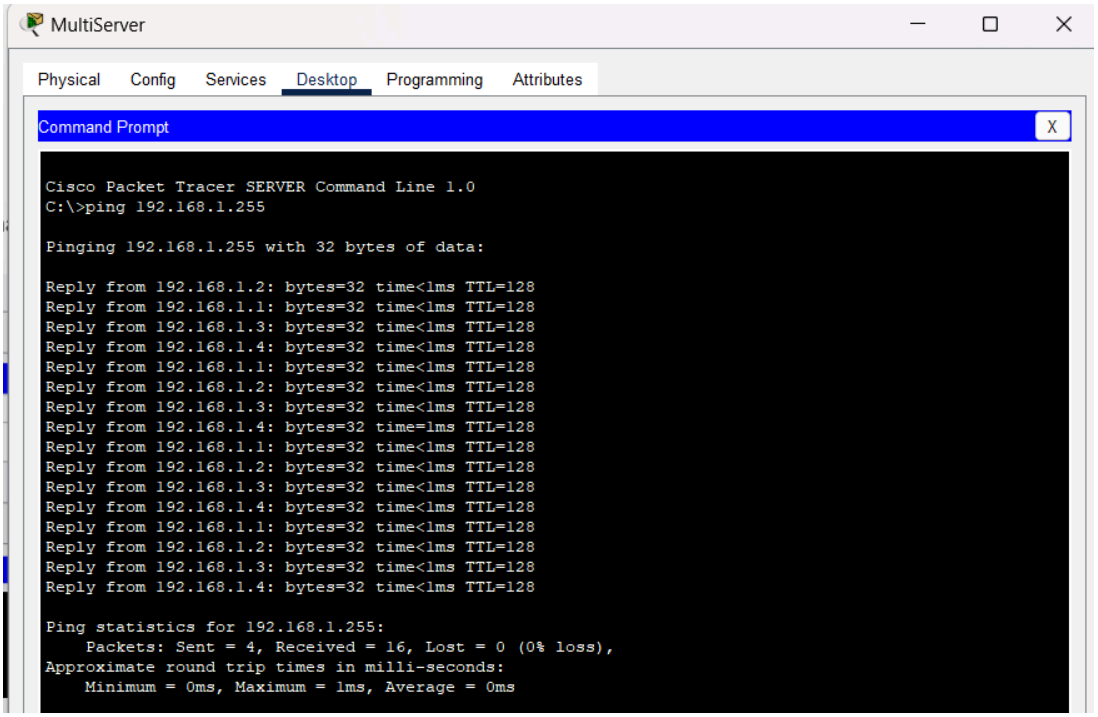
BÁO CÁO LAB-5 INT2213_20

Hà Đăng Long 22024552

Part 1: Generate Network Traffic in Simulation Mode

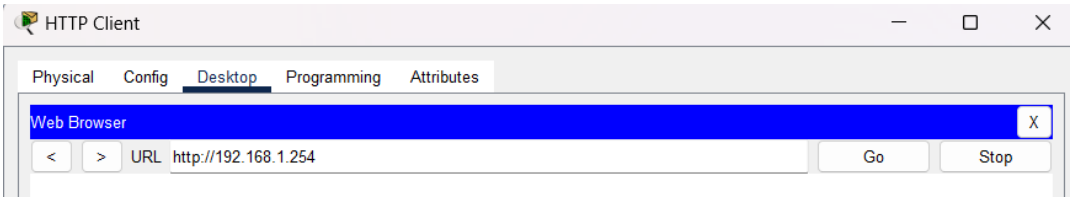
1. **Tạo lưu lượng để điền bảng ARP (Address Resolution Protocol):**

Bằng cách sử dụng lệnh ping, tất cả các thiết bị trong mạng sẽ phản hồi lại, giúp điền vào bảng ARP.



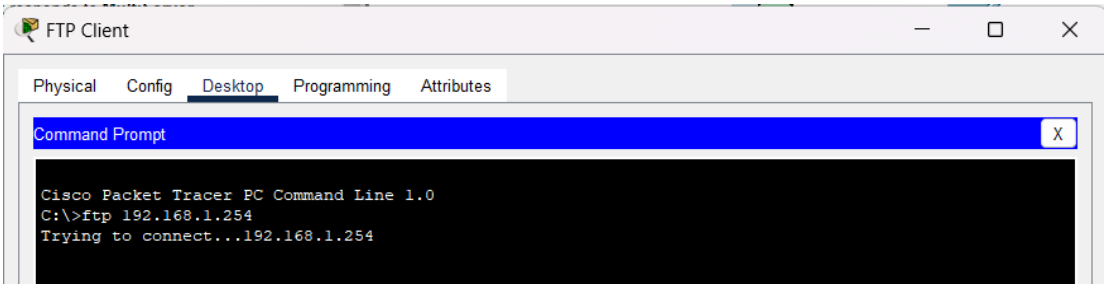
2. **Tạo lưu lượng web (HTTP):**

Bằng cách truy cập một trang web thông qua HTTP Client, bạn tạo ra lưu lượng mạng HTTP.



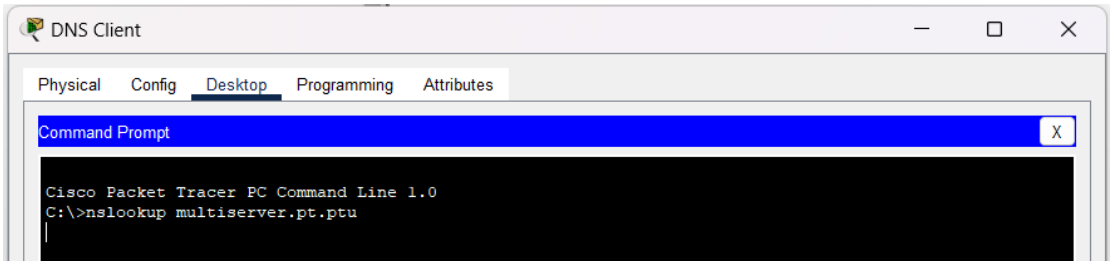
3. **Tạo lưu lượng FTP (File Transfer Protocol):**

Khi bạn kết nối đến một máy chủ FTP, bạn tạo ra lưu lượng mạng FTP.



4. **Tạo lưu lượng DNS (Domain Name System):**

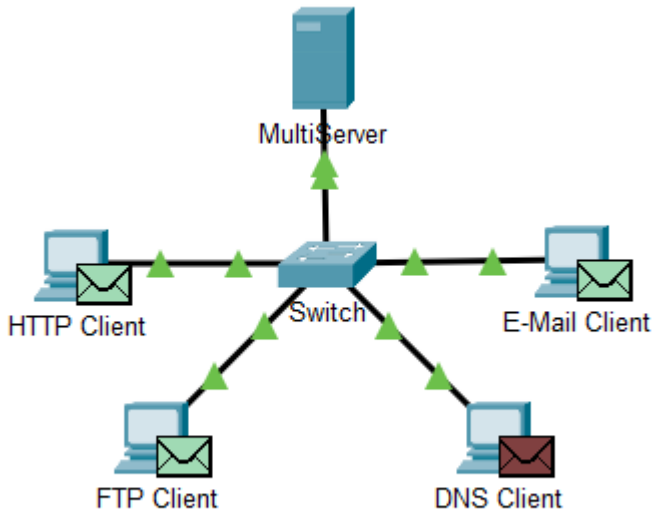
Khi bạn sử dụng lệnh nslookup để tra cứu tên miền, bạn tạo ra lưu lượng mạng DNS.



5. **Tạo lưu lượng Email:**

Khi bạn gửi một email, bạn tạo ra lưu lượng mạng Email.

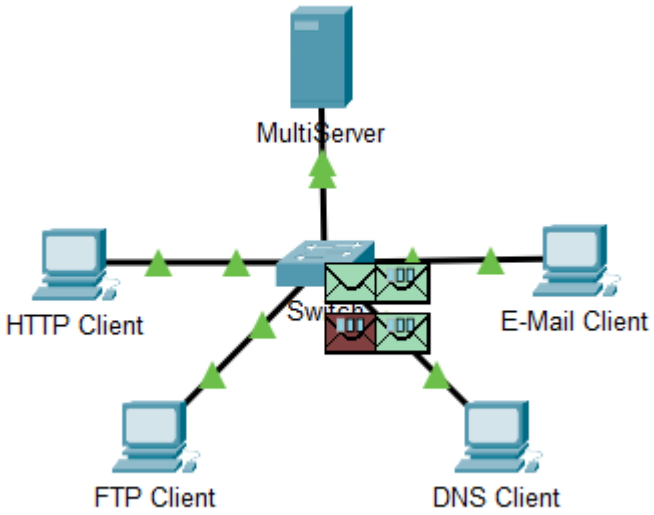
6. **Xác minh rằng lưu lượng đã được tạo và sẵn sàng cho mô phỏng:**



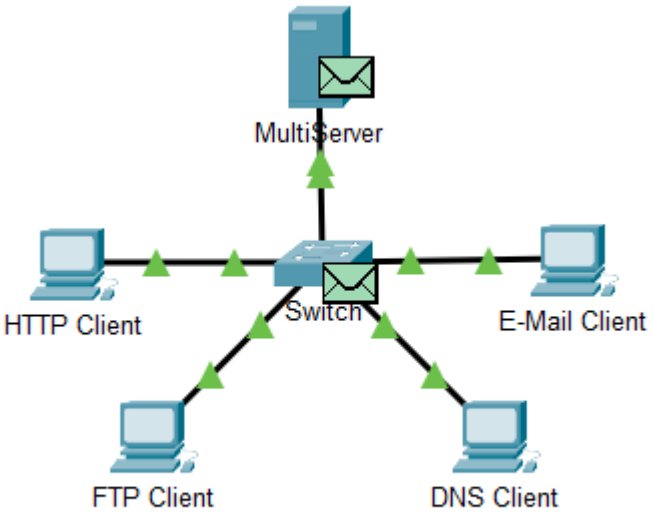
Part 2: Examine Functionality of the TCP and UDP Protocols

1. **Kiểm tra multiplexing các lưu lượng mạng đi qua**

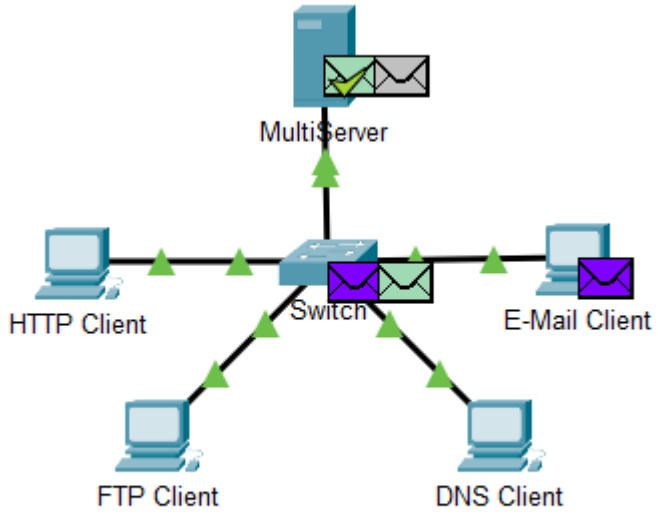
a. Bấm foward 1 lần. Tất cả các PDU được chuyển tới switch



b. Tiếp tục bấm foward 1 lần. Một số PDU đã biến mất vì các PDU đó đã được lưu trữ trong switch



c. Tiếp tục bấm foward 6 lần. Tất cả clients đều nhận được phản hồi. Chú ý rằng chỉ 1 PDU được đi qua mỗi hướng tại 1 thời điểm. Điều này được gọi là Multiplexing



d. Một loạt các PDU xuất hiện trong danh sách sự kiện ở góc trên bên phải của cửa sổ mô phỏng. Có rất nhiều màu sắc tại đây vì mỗi màu biểu diễn các giao thức khác nhau

2. Khám phá lưu lượng truy cập HTTP khi các máy khách giao tiếp với máy chủ.

a. Lọc lưu lượng truy cập hiện tại để chỉ hiển thị HTTP và TCP PDUs.
b. Nhấp vào nút Capture/Forward. Di chuyển chuột của bạn trên mỗi PDU cho đến khi bạn tìm thấy một PDU xuất phát từ HTTP Client. Nhấp vào phong bì PDU để mở nó.
c. Nhấn vào *Inbound PDU Details* và lướt xuống cuối. Phần được dán nhãn gọi là TCP. Giao tiếp này là đáng tin cậy
d. Ghi lại các giá trị SRC PORT, DEST PORT, SEQUENCE NUM, và ACK NUM. Đây là thứ được viết ở bên trái WINDOW: 1025, 80, 0, 0. SYN.
e. Đóng PDU vào bấm foward
f. Bấm vào PDU envelope và chọn PDU Inbound Details. Đây là sự khác biệt:

SYN has changed to SYN+ACK as acknowledgement number is 1, SOURCE PORT: 80 and DESTINATION PORT: 1025.

h. What information is now listed in the TCP section? How are the port and sequence numbers different from the previous two PDUs?

1025,80,1,1. SYN+ACK has changed to PSH+ACK. Source and destination port exchanged and sequence and acknowledgement numbers are both 1.

3. Khám phá lưu lượng truy cập FTP khi các máy khách giao tiếp với máy chủ.

c. Click the Inbound PDU Details tab and scroll down to the last section. What is the section labeled ?
TCP
Are these communications considered to be reliable?
YES

d. Record the SRC PORT, DEST PORT, SEQUENCE NUM, and ACK NUM values. What is written in the field to the left of the WINDOW field?
1025, 21, 0, 0. SYN

f. Click the PDU envelope and select Inbound PDU Details. How are the port and sequence numbers different than before?
21, 1025, 0, 1. SYN+ACK

g. Click the Outbound PDU Details tab. How are the port and sequence numbers different from the previous two results?
1025, 21, 1, 1. ACK. Source and destination port exchanged and sequence and acknowledgement numbers are both 1.

i. Open the PDU and select Inbound PDU Details. Scroll down past the TCP section. What is the message from the server?
Welcome to PT Ftp server.

4. Khám phá lưu lượng truy cập DNS khi các máy khách giao tiếp với máy chủ.
c.Click the Inbound PDU Details tab and scroll down to the last section. What is the section labeled?
UDP

d. Record the SRC PORT and DEST PORT values. Why is there no sequence and acknowledgement number?
SRC PORT: 1025, DEST PORT: 53. UDP does not need to establish a reliable connection.

f. Click the PDU envelope and select Inbound PDU Details. How are the port and sequence numbers different than before?
SRC PORT: 53, DEST PORT:1025. Reversed port number.

g.What is the last section of the PDU called
DNS Answer

5. Khám phá lưu lượng truy cập email khi các máy khách giao tiếp với máy chủ.

c. Click the Inbound PDU Details tab and scroll down to the last section. What transport layer protocol does email traffic use?
TCP

Are these communications considered to be reliable?
YES

d. Record the SRC PORT, DEST PORT, SEQUENCE NUM, and ACK NUM values. What is written in the field to the left of the WINDOW field?
1025, 25, 0, 0. SYN.

f. Click the PDU envelope and select Inbound PDU Details. How are the port and sequence numbers different than before?
25, 1025, 0, 1. SYN+ACK. Source and destination port exchanged and sequence and acknowledgement numbers are both 1.

g. Click the Outbound PDU Details tab. How are the port and sequence numbers different from the previous two results?
1025, 25, 1, 1. ACK. Source and destination port exchanged and sequence and acknowledgement numbers are both 1.

i. How are the port and sequence numbers different from the previous two PDUs?
1025, 25, 1, 1. PSH+ACK. Source and destination port exchanged and sequence and acknowledgement numbers are both 1.

6. Khám phá việc sử dụng số cổng từ máy chủ.

b. Enter the netstat command. What protocols are listed in the left column?

What port numbers are being used by the server?
21

c. What states are the sessions in?
ESTABLISHED

d. Repeat the netstat command several times until you see only one session still ESTABLISHED. For which service is this connection still open?
FTP

Why doesn't this session close like the other three?
Server waiting for Username.