

Lab 01: MẠNG ETHERNET

Thông tin Frame Ethernet:

Ethernet frame structure

```

.....+-----+-----+-----+-----+-----+-----+.....
.(Pre.)| dest.  | source | Eth.  | data   | (CRC) |
      | addr.  | addr.  | type  |        |       |
.....+-----+-----+-----+-----+-----+-----+.....

```

```
Some Eth. types: 0x0200 = XEROX PUP  
                  0x0800 = DoD Internet (IPv4)  
                  0x0806 = ARP  
                  0x8035 = RARP
```

Thông tin Frame ARP:

ARP frame structure

```
+16b-+-16b-+8b+8b+16b+-lgHW-+-lgP-+-lgHW-+-lgP-+
|HW   |Proto|HW|P  |Op.|AddrHW|AddrP|AddrHW|addrP|
|Type|Type |lg|lg|   |Source|Src.  |Rcpt.  |Rcpt.  |
+---+-----+-----+-----+-----+-----+-----+-----+
```

```
Some types: 0x0001 = Ethernet
             0x0800 = DoD Internet (IPv4)
Operations (Op.): 0x0001 = Request
                  0x0002 = Answer
```

Thông tin gói tin IPv4:

IPv4 packet structure

```

<-----32bits----->
<-4b->      <--8bits--><-----16bits----->
+-----+-----+-----+-----+
| Ver | IHL | TOS          | Total Length (Bytes) |
+-----+-----+-----+-----+
| Identifier          | Fl | F0          |
+-----+-----+-----+-----+
| TTL          | Protocol | Checksum (header) |
+-----+-----+-----+-----+
| Source Address                                     |
+-----+-----+-----+-----+
| Destination Address                               |
+-----+-----+-----+-----+
...      Options
+-----+-----+-----+-----+
...      Data
+-----+-----+-----+-----+

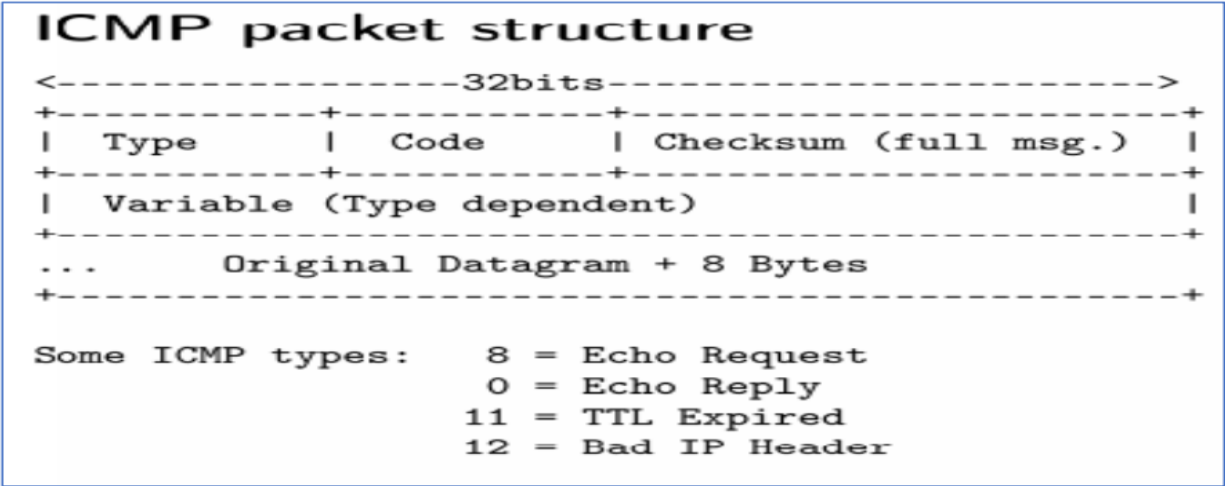
```

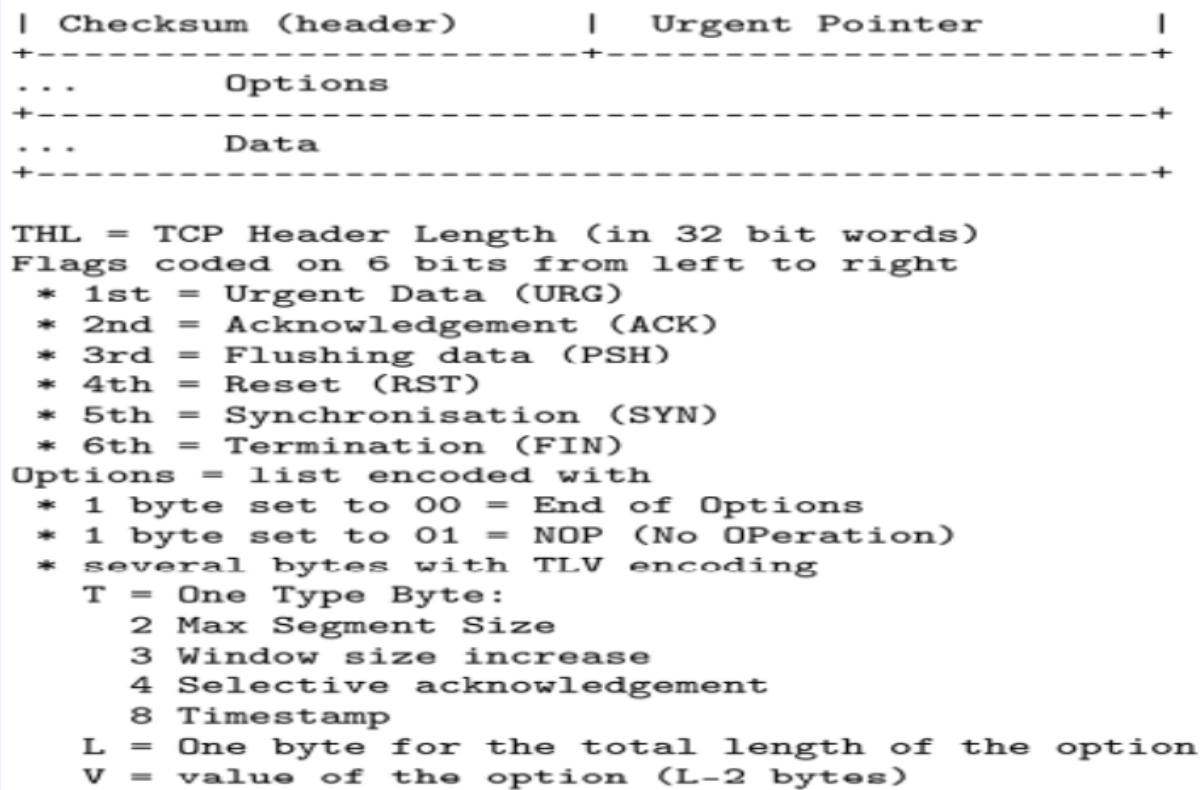
Ver = IP Version
 IHL = IP Header Length (in 32 bit words)
 TOS = Type Of Service
 Fl (3 first bits) = Fragmentation Bits
 * 1st = Reserved
 * 2nd = Don't Fragment
 * 3rd = More Fragments
 FO (13 following bits) = Fragment Offset
 TTL = Time to Live
 Some Protocols:

8	=	EGP
11	=	GLOUP
17	=	UDP
46	=	RSVP

1	=	ICMP
4	=	IP (encapsulation)
6	=	TCP

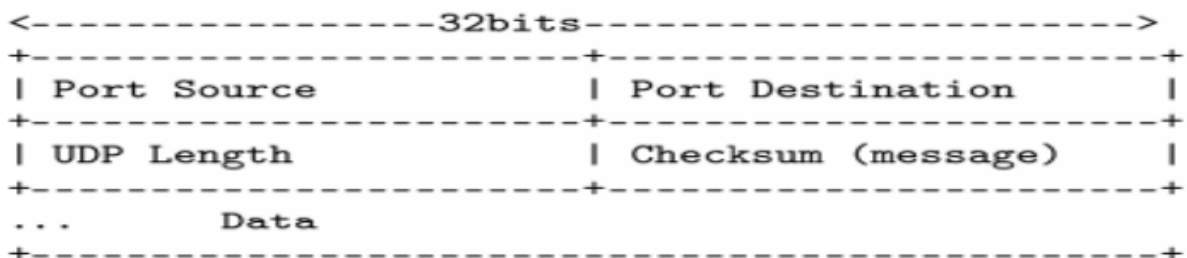
Thông tin gói tin ICMP:





Thông tin về UDP

UDP datagram structure



Port number associated services

ftp-data	20/tcp		
ftp	21/tcp		
ssh	22/tcp	ssh	22/udp
telnet	23/tcp		
smtp	25/tcp		
domain	53/tcp	domain	53/udp
		tftp	69/udp
www	80/tcp	www	80/udp
kerberos	88/tcp	kerberos	88/udp
pop-3	110/tcp	pop-3	110/udp
		snmp	161/udp
		snmp-trap	162/udp

Bài tập 1: Phân tích Frame bằng cách tìm các trường thông tin sau:

	MAC đích	MAC nguồn	IPv4 Ver
0000	b0 be 76 df cc 34	00 08 ca 33 69 fa	08 00 45 00 ..v..4...3i...E.
	010 0 0000 0000 0000		
0010	00 28 2e b7 40 00 80 06	46 0d c0 a8 00 65 ac d9	.(..@...F....e..
	0101 0000 0001 0000		
0020	18 25 d2 27 01 bb 3d 78	3a 68 d4 37 32 bb 50 10	.%!...=x:h.72.P.
0030	20 2b b6 e7 00 00		+....

- Địa chỉ MAC đích là bao nhiêu: b0 be 76 df cc 34
Hãy cho biết số OUI của vendor nào: _____
- Địa chỉ MAC nguồn là bao nhiêu: 00 08 ca 33 69 fa
Hãy cho biết số OUI của vendor nào: _____
- Ethernet Frame có Type là gì: IPv4

Nếu Frame là IP hãy phân tích tiếp các trường sau:

- Version: 4
- IHL: 5
- TOS: 00
- Total Length: 00 28
- Identifier: 2e b7
- F1: 010 Don't Fragment
- F0: 0 0000 0000 0000
- TTL: 80 = $8 \cdot 16^1 + 0 \cdot 16^0 = 128$
Dựa trên số TTL hãy dự đoán hệ điều hành của gói tin này bằng bảng 1.
Hệ điều hành dự đoán: Windows XP, 7, 8
- Protocol: 06h = 6(10)
- CheckSum: 46 0d
- Source Address (hệ 10): 192.168.0.101
- Destination Address (hệ 10): 172.217.24.37

Nếu là ICMP hãy cho biết đây là ICMP Request hay Response

.....

Nếu là TCP hãy cho biết các trường sau:

- Source Port (hệ 10): 53799
- Destination Port (hệ 10): 443
- Sequence Number: 3d 78 3a 68
- Acknowledgment Number: d4 37 32 bb
- Flag: (cho biết cờ nào đang bật) ACK (01 0000)
- Windows Size: 20 2b

Nếu là UDP hãy cho biết các trường sau:

- Port Source: _____
- Port Destination: _____

Lưu ý: nếu Port Source hoặc Port Dest có vùng port nằm trong bảng Port Number Associated Services, sinh viên hãy cho biết service liên quan là service nào

Bài tập 2: Hãy phân tích Frame sau với yêu cầu tương tự bài tập 1:

```
0000  b0 be 76 df cc 34 00 08 ca 33 69 fa 08 00 45 00  ..v..4...3i...E.
0010  00 3d d1 ad 40 00 80 11 d8 ba c0 a8 00 65 4a 7d  .=-.@.....eJ}
0020  44 bd cc ce 01 bb 00 29 08 3d 48 97 06 83 9f 28  D.....).=H....(
0030  48 1c 1c d9 cf 76 18 32 ad 19 85 14 b9 af cc dc  H....v.2.....
0040  27 ea 0e 3c df 87 68 0c 10 37 57                '..<..h..7W
```

Sinh viên trả lời vào form Bài tập 2. (Link: <https://forms.gle/PEiYZnRy3cFuud5Q9>)

Bài tập 3: Hãy phân tích Frame sau với yêu cầu tương tự bài tập 1:

```

0000  b0 be 76 df cc 34 00 08 ca 33 69 fa 08 00 45 00  ..v..4...3i...E.
0010  00 3c 28 16 00 00 80 01 41 8e c0 a8 00 65 08 08  .<(...A....e..
0020  08 08 08 00 4d 2e 00 01 00 2d 61 62 63 64 65 66  ....M....-abcdef
0030  67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76  ghijklmnopqrstuv
0040  77 61 62 63 64 65 66 67 68 69                      wabdefghi

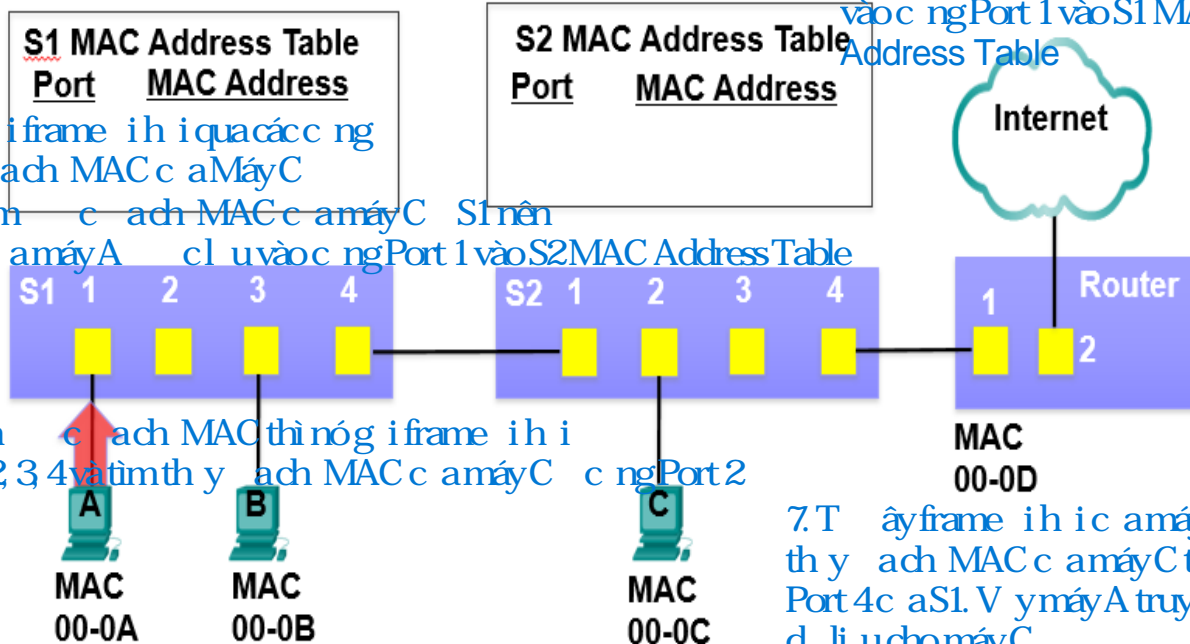
```

Sinh viên trả lời vào form Bài tập 3. (Link:

<https://forms.gle/PEiYZnRy3cFuud5Q9>)

Bài tập 4: Mô tả hoạt động của mạng sau:

1. Máy tính A gửi frame tới Switch S1
 2. Khi S1 nhận được frame thì nó sẽ tìm kiếm địa chỉ MAC của máy A trong bảng địa chỉ MAC của S1.
 3. Khi S1 không tìm thấy địa chỉ MAC của máy A trong bảng địa chỉ MAC của S1 thì nó sẽ gửi frame tới tất cả các cổng (flooding).
 4. Khi S1 gửi frame tới tất cả các cổng thì nó sẽ nhận được phản hồi từ máy A qua cổng 1.
 5. Khi S1 nhận được phản hồi từ máy A qua cổng 1 thì nó sẽ cập nhật địa chỉ MAC của máy A vào bảng địa chỉ MAC của S1.
 6. Khi S1 nhận được frame từ máy A qua cổng 1 thì nó sẽ gửi frame tới máy C qua cổng 4.
 7. Khi S2 nhận được frame từ S1 qua cổng 1 thì nó sẽ tìm kiếm địa chỉ MAC của máy C trong bảng địa chỉ MAC của S2.
 8. Khi S2 không tìm thấy địa chỉ MAC của máy C trong bảng địa chỉ MAC của S2 thì nó sẽ gửi frame tới tất cả các cổng (flooding).
 9. Khi S2 gửi frame tới tất cả các cổng thì nó sẽ nhận được phản hồi từ máy C qua cổng 2.
 10. Khi S2 nhận được phản hồi từ máy C qua cổng 2 thì nó sẽ cập nhật địa chỉ MAC của máy C vào bảng địa chỉ MAC của S2.
 11. Khi S2 nhận được frame từ S1 qua cổng 1 thì nó sẽ gửi frame tới Router qua cổng 1.
 12. Khi Router nhận được frame từ S2 qua cổng 1 thì nó sẽ gửi frame tới Internet qua cổng 2.



3 Khi S1 gửi frame tới tất cả các cổng
 2, 3, 4 thì nó sẽ nhận được phản hồi từ máy C qua cổng 2.

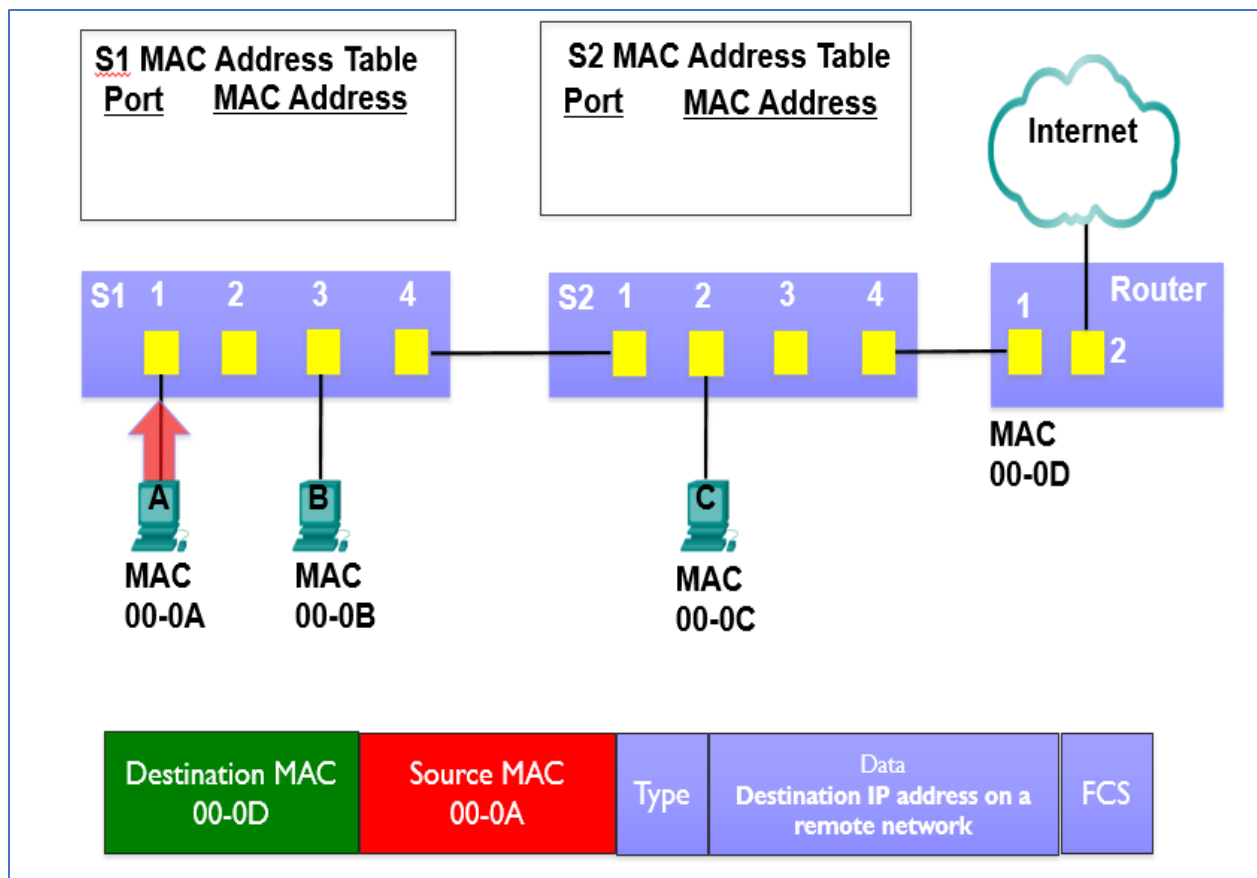
4 Do không tìm thấy địa chỉ MAC của máy C trong bảng địa chỉ MAC của S1 nên S1 sẽ gửi frame tới tất cả các cổng (flooding).
 5 Khi S1 gửi frame tới tất cả các cổng thì nó sẽ nhận được phản hồi từ máy A qua cổng 1.

6 Khi S2 nhận được frame từ S1 qua cổng 1 thì nó sẽ tìm kiếm địa chỉ MAC của máy C trong bảng địa chỉ MAC của S2.
 7. Khi S2 không tìm thấy địa chỉ MAC của máy C trong bảng địa chỉ MAC của S2 thì nó sẽ gửi frame tới tất cả các cổng (flooding).
 8. Khi S2 gửi frame tới tất cả các cổng thì nó sẽ nhận được phản hồi từ máy C qua cổng 2.

7. Khi S2 nhận được frame từ S1 qua cổng 1 thì nó sẽ tìm kiếm địa chỉ MAC của máy C trong bảng địa chỉ MAC của S2.
 8. Khi S2 không tìm thấy địa chỉ MAC của máy C trong bảng địa chỉ MAC của S2 thì nó sẽ gửi frame tới tất cả các cổng (flooding).
 9. Khi S2 gửi frame tới tất cả các cổng thì nó sẽ nhận được phản hồi từ máy C qua cổng 2.

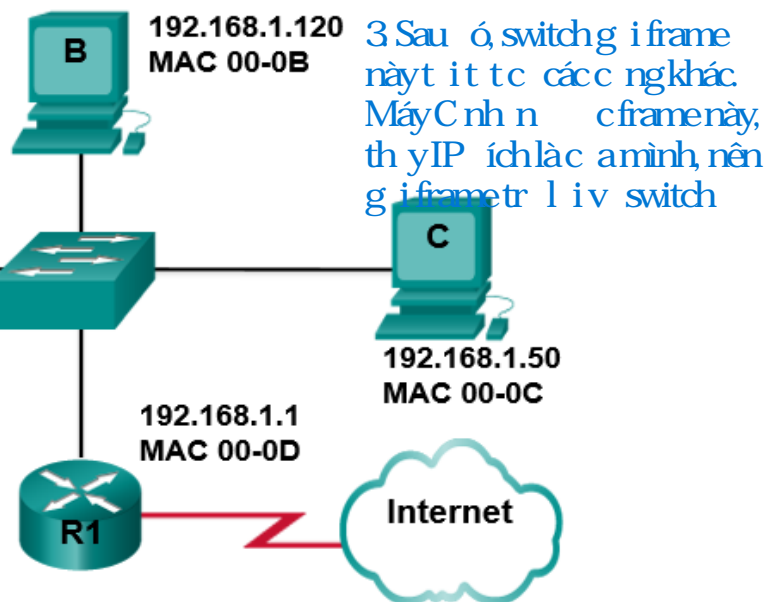
6 Lúc này, địa chỉ MAC của máy C đã được cập nhật vào bảng địa chỉ MAC của S1 qua cổng 1. Khi S1 nhận được frame từ máy A qua cổng 1 thì nó sẽ gửi frame tới máy C qua cổng 4.

Destination MAC 00-0C	Source MAC 00-0A	Type	Data Destination IP address on a remote network	FCS
--------------------------	---------------------	------	--	-----



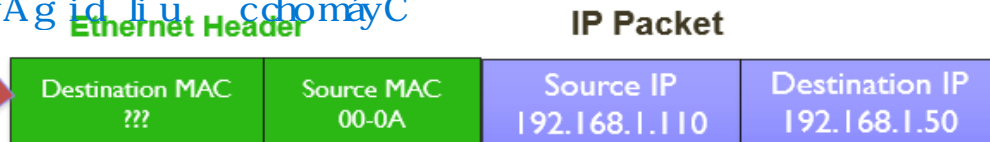
Bài tập 5: Mô tả hoạt động của mạng sau (có giao thức ARP)

1. Lúc đầu, máy A không biết địa chỉ MAC của máy C. Nó chỉ biết địa chỉ IP của máy C.
2. Máy A gửi frame ARP Broadcast tới switch, switch lưu địa chỉ MAC của máy A và gửi nó vào MAC Address Table.



4. Sau khi nhận được, Switch lưu địa chỉ MAC của máy C vào bảng MAC và gửi frame trả lại cho máy A.

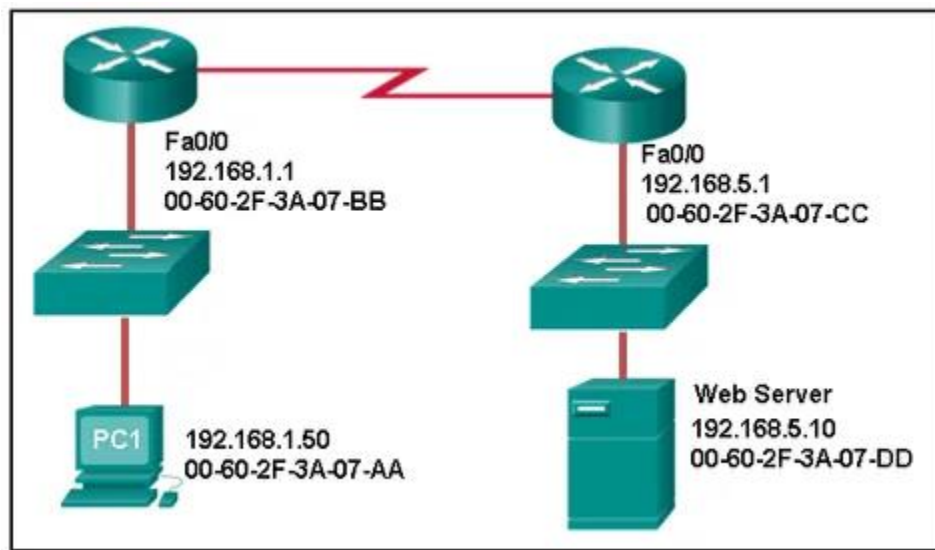
5. Sau khi máy A nhận được frame trả lại có địa chỉ MAC đích là 00-0C, địa chỉ nguồn là 00-0A, nó gửi qua switch. Switch tra bảng MAC, thấy địa chỉ là máy C nên chuyển frame cho máy C. Máy C nhận được frame. Tiếp theo máy A gửi dữ liệu cho máy C.



Bài tập 6: Sinh viên mở Lab 6 trong Folder Packet Tracer để làm bài tập.

Bài tập 7: Trả lời các câu hỏi sau:

Câu 1: Dựa trên hình sau. Địa chỉ MAC đích của Frame Ethernet là gì khi nó rời khỏi máy chủ web nếu đích cuối cùng là PC1



Trả lời: 00-60-2F-3A-07-AA

Câu 2: Lệnh nào để xem địa chỉ MAC trên máy tính, Switch. Thêm, xóa địa chỉ MAC vào ARP Cache. Nêu tác dụng của ARP Cache.

Trả lời:

Bài tập 8: Bấm cáp mạng 586A và 586B

Sinh viên nộp hình sản phẩm bấm cáp theo 2 chuẩn vào bài tập này.