LABORATORIO DIDATTICO 3

Creazione ed invio di frame e pacchetti con packETH

Si propone l'utilizzo del pacchetto software **packETH** in ambiente LINUX[1] UBUNTU per approfondire la conoscenza dei protocolli Ethernet e ARP attraverso la creazione frame Ethernet II che trasportano pacchetti del protocollo ARP.

Se la rete non è di vostra proprietà, o non ne siete amministratori, prima di procedere chiedete l'autorizzazione scritta all'amministratore di rete.

L'obiettivo di questo LABORATORIO DIDATTICO è quello di comprendere la struttura di un frame Ethernet e la funzione del protocollo ARP, il quale permette di effettuare la risoluzione degli indirizzi IP in indirizzi MAC (detti anche indirizzi fisici o indirizzi hardware), cioè di ricercare l'indirizzo MAC associato all'indirizzo IP di un'interfaccia Ethernet presente in una LAN.
Consideriamo una LAN Ethernet di piccole dimensioni (FIGURA 1), costituita da alcuni computer, da uno switch e da un router tramite cui si accede a Internet (il router funge da *gateway*, cioè da punto di uscita). Per la comunicazione in rete i computer adottano la *suite di protocolli TCP/IP*.
L'interfaccia Ethernet del router abbia **indirizzo IP 10.0.0.1** (con subnet mask 255.255.255.0).
Da un PC avente **indirizzo IP 10.0.0.10** (con subnet mask 255.255.255.0) desideriamo creare dei frame Ethernet e verificare il principio di funzionamento del protocollo ARP.
Il protocollo ARP ha il compito di ricercare all'interno di una LAN Ethernet l'indirizzo MAC associato al'indirizzo IP di una determinata interfaccia di rete Ethernet, in modo da poterlo utilizzare come indirizzo MAC di destinazione quando si deve inviare un frame alla macchina che ha tale interfaccia Ethernet.
Per esempio, come si vedrà meglio nei capitoli successivi, per verificare se una determinata macchina di cui si conosce l'indirizzo IP (o il nome host) è collegata in rete ed è operativa è possibile utilizzare (da prompt dei comandi in ambiente Windows o da terminale in ambiente Linux) il comando: **ping <indirizzo IP>**.
Prima di effettuare il ping, però, il computer utilizza il protocollo **ARP** per cercare l'indirizzo MAC associato all'indirizzo IP 10.0.0.1; sintetizzando, il protocollo ARP opera nel seguente modo:

1. il protocollo ARP crea un pacchetto (o PDU) ARP di richiesta (ARP Request) contenente come *Target* l'indirizzo IP associato all'indirizzo MAC da cercare (il *Target MAC* è genericamente indicato da 48 zeri, aventi il significato di "indirizzo non specificato");
2. il pacchetto ARP di richiesta viene incapsulato nel campo *data* di un frame Ethernet, nel cui header si inseriscono: l'indirizzo MAC di destinazione di **Broadcast** (tutti 1, ff:ff:ff:ff:ff:ff in esadecimale), l'indirizzo MAC sorgente (quello della scheda Ethernet del PC, si ricorda che i primi 3 byte identificano il costruttore), il tipo di protocollo dello strato 3 che sta operando (il protocollo ARP identificato in esadecimale, 0x, dal numero 0806); viene quindi inserito automaticamente il preambolo (101010...1011), e sono calcolati i 4 byte (32 bit) da inserire nel campo di coda FCS (Frame Check Sequence) per consentire la rivelazione d'errore attraverso un metodo denominato CRC (*Cyclic Redundancy Check*);
3. il frame viene quindi inviato in rete tramite lo strato fisico dell'interfaccia Ethernet e giunge a tutte le macchine in rete;
4. la macchina che riconosce nome proprio l'indirizzo IP *Target*, contenuto nella richiesta ARP, risponde con un pacchetto ARP di risposta (**ARP replay**) in cui viene inserito come indirizzo sorgente l'indirizzo MAC cercato;
5. il pacchetto ARP di risposta viene inserito in un frame avente come indirizzo MAC di destinazione quello della scheda Ethernet del computer che aveva inviato la richiesta ARP;
6. l'indirizzo MAC così ottenuto viene memorizzato temporaneamente nella *cache ARP* del computer;
7. a questo punto è possibile avviare la procedura che effettua il *ping* vero e proprio.

[1] PackETH è disponibile anche in versione Windows.

Per questo LABORATORIO DIDATTICO è consigliabile operare in ambiente **Linux Ubuntu**, installando i seguenti pacchetti software:

- **packETH** (http://packeth.sourceforge.net), software per la creazione e l'invio in rete di frame Ethernet in grado di trasportare diversi tipi di protocolli e di traffico;
- analizzatore di protocollo **Wireshark** (www.wireshark.org), installabile direttamente tramite *Ubuntu Software Center* (o *Synaptic* o da terminale con *sudo apt-get install wireshark*);

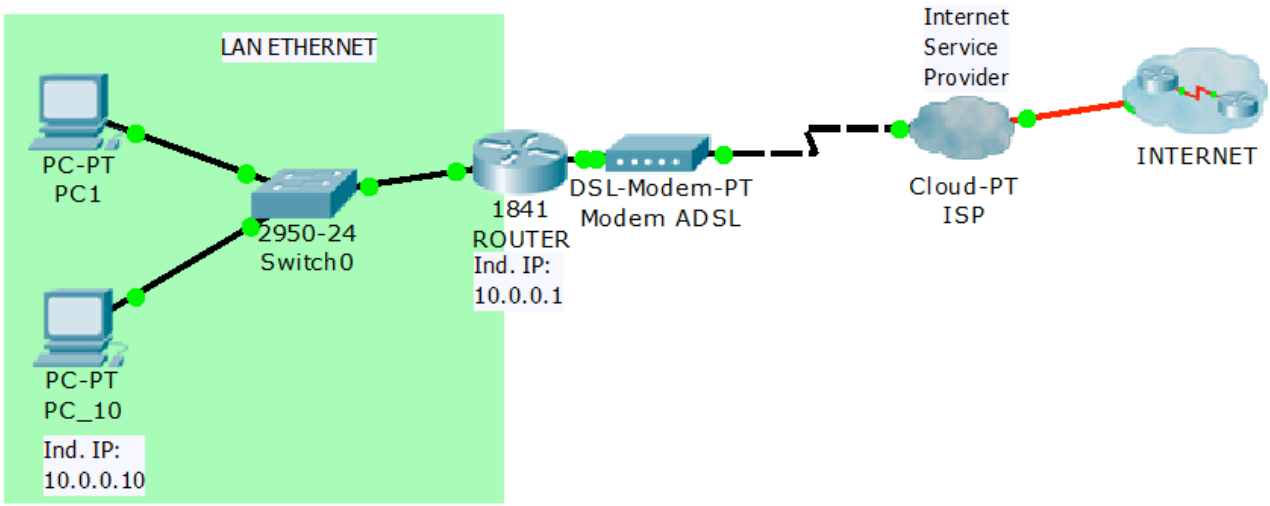

FIGURA 1 LAN Ethernet con accesso a Internet (simulata con Cisco Packet Tracer)

In questa esercitazione si è utilizzata la versione 1.7.3 di packETH che è stata installata su un PC con s.o. Ubuntu (12.04) partendo dai sorgenti, operando nel seguente modo:

- dal sito di packETH (http://packeth.sourceforge.net) scarichiamo il file compresso contenente i sorgenti, li decomprimiamo (viene creata la cartella packETH-1.7.3).
- Come prima cosa installiamo le librerie **libgtk-3-dev** e **libglib2.0-dev**. (da terminale con sudo apt-get install libgtk-3-dev libglib2.0-dev o tramite il Gestore pacchetti).
- Con i diritti di amministratore ci spostiamo nella cartella packETH-1.7.3 ed eseguiamo il processo di installazione da terminale, digitando i comandi: **sudo ./configure**; **sudo make**; **sudo make install**.

In alternativa è possibile installare in modo più semplice una versione precedente di packETH (la 1.6 al momento della stesura del testo) tramite *Gestore di pacchetti* (o *Ubuntu Software Center*) e inserendo **packeth** nella barra di ricerca: di seleziona il programma e lo si fa installare automaticamente.

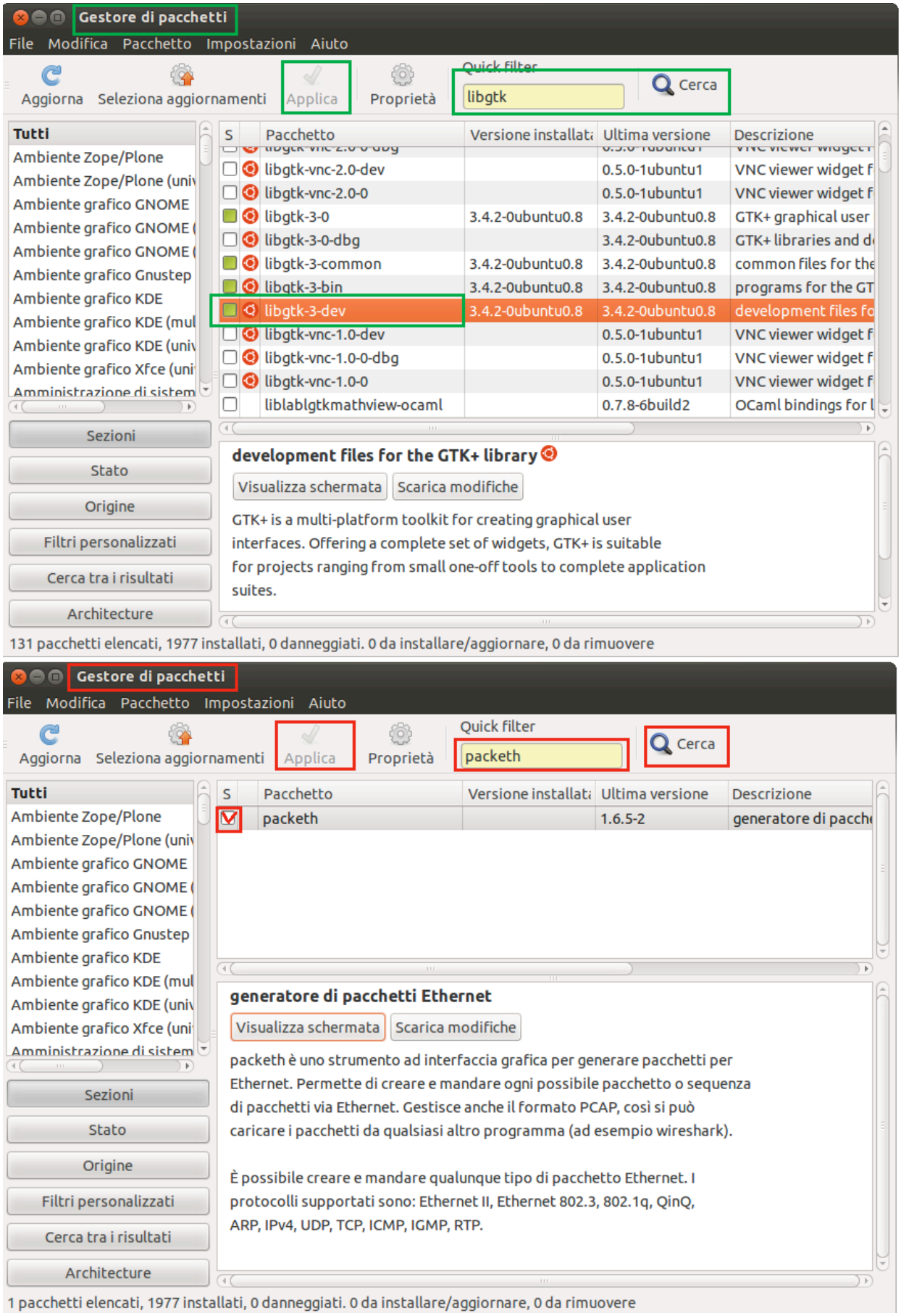

FIGURA 2 Installazione di packeth tramite il Gestore Pacchetti di Ubuntu.

Eseguita l'installazione apriamo packETH da terminale (con i diritti di amministratore) con il comando: **sudo packETH**.
Se si è eseguita l'installazione automatica da Gestore di pacchetti si può digitare semplicemente: **sudo packeth**.
Ricordarsi che l'ambiente LINUX è *case sensitive* per cui è necessario digitare le minuscole e le maiuscole che compongono il nome del programma[2].

Per evitare di dover digitare ogni volta gli indirizzi IP e gli indirizzi MAC delle varie macchine in rete è possibile creare ed utilizzare un file di testo con funzione di database, denominato **addresslist**, che nella versione 1.7 viene caricato automaticamente se si fa partire packETH dalla directory di installazione (nella versione 1.6 si può selezionare il file di testo che funge da database cliccando su **File, select database**). Il file può essere editato direttamente da packETH 1.7, cliccando su **select** nel menu Builder, oppure utilizzando un editor di testo e inserendo una riga per ogni macchina contenente:<indirizzo IPv4>,<indirizzo IPv6>,<indirizzo MAC>,<nome host> (l'indirizzo IPv6 può essere omesso se non viene utilizzato). In FIGURA 3 si mostra la schermata di packETH che compare una volta lanciato il programma.
Il menu **Builder** ci permette di creare un frame Ethernet II e il pacchetto di **ARP request** da esso trasportato (FIGURA 3):

- selezioniamo **ver II** (Ethernet versione II) per scegliere il protocollo dello strato 2 OSI (*Link Layer*) di cui vogliamo creare un frame e inseriamo i valori relativi ai campi dell'header: *Destination* (MAC address) <ff:ff:ff:ff:ff:ff> (*broadcast*); *Source* (MAC address), indirizzo MAC della scheda Ethernet del nostro computer (rilevabile tramite il comando **ifconfig** nel cui output è indicato come hardware address); *EtherType*, selezioniamo ARP (identificato dal numero esadecimale (0x) 0806;
- passiamo a definire le caratteristiche del pacchetto ARP, scegliendo il tipo di messaggio (operazione): *ARP Request*, inserendo come Sender MAC (address) e Sender IP (address) l'indirizzo MAC e l'indirizzo IP della scheda di rete del nostro computer; come Target MAC (address) 00:00:00:00:00:00 (tutti 0, indirizzo non specificato) e come Target IP (address) l'indirizzo IP dell'interfaccia Ethernet associato all'indirizzo MAC richiesto (il valore *HW type* indica Ethernet, quello *HW size* indica la dimensione in byte dell'indirizzo MAC (6 byte, 48 bit); il valore *Protocol type* indica IPv4, quello *Prot. size* indica la dimensione in byte dell'indirizzo IPv4 (4 byte, 32 bit).

[2] Può essere utile verificare che il file eseguibile sia presente anche nella cartella usr/local/bin o in /usr/bin (per l'installazione con Gestore dei pacchetti); in caso contrario andare nella cartella di pachETH e digitare il comando **sudo ./packETH** per eseguirlo direttamente da tale cartella.

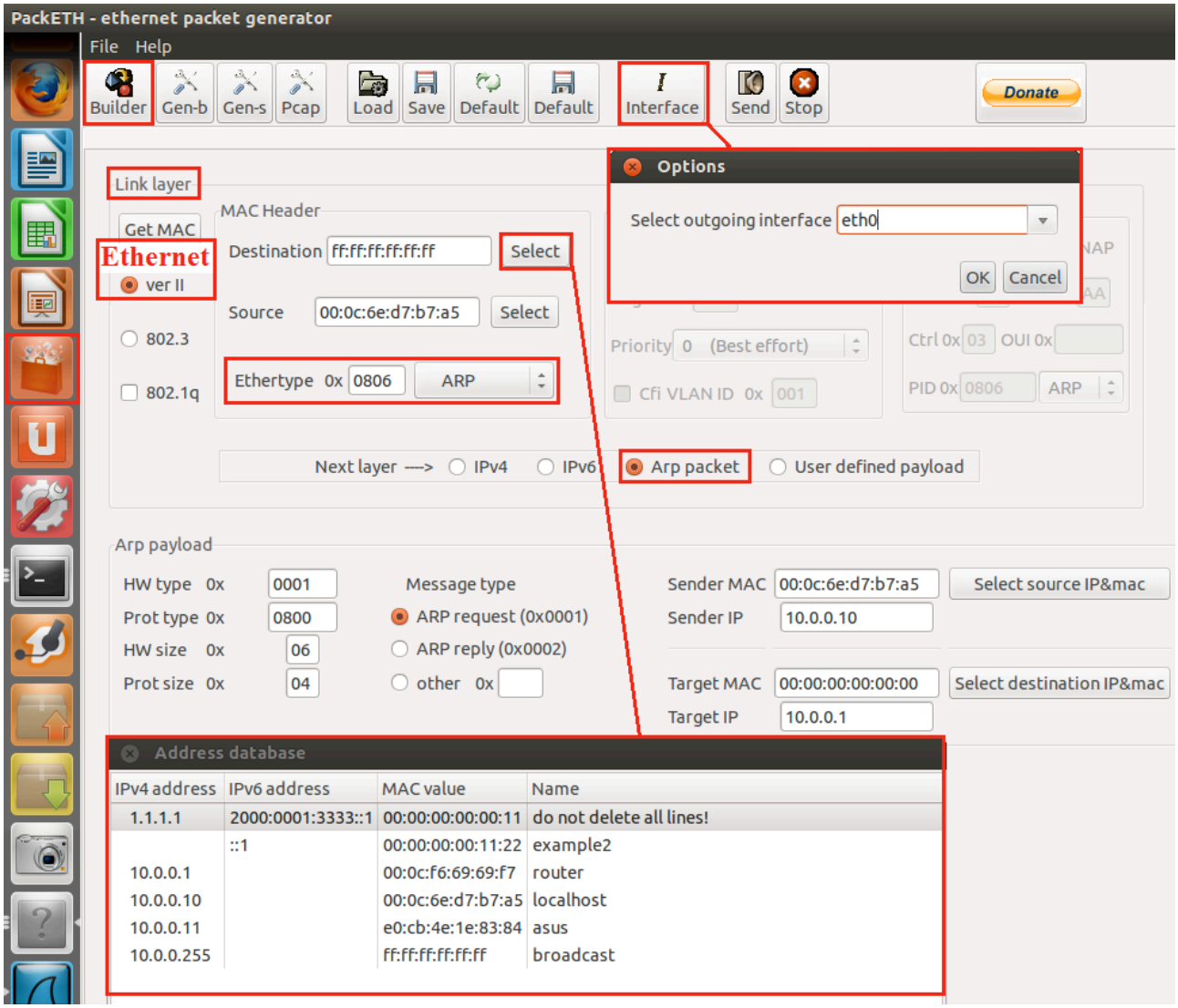

FIGURA 3 Menu Builder di PackETH

Cliccando su **Gen-b** possiamo scegliere il numero di pacchetti (e quindi di frame) da inviare, per esempio 5, e la velocità alla quale inviarli, FIGURA 4. Il programma calcola automaticamente, con il metodo del CRC, i 4 byte (espressi in esadecimale, 0x) da inserire nel campo di coda FCS che consente la rivelazione degli errori.
Clicchiamo quindi su **Interface** per scegliere l'interfaccia fisica (Ethernet, Eth0) su cui inviare i frame.

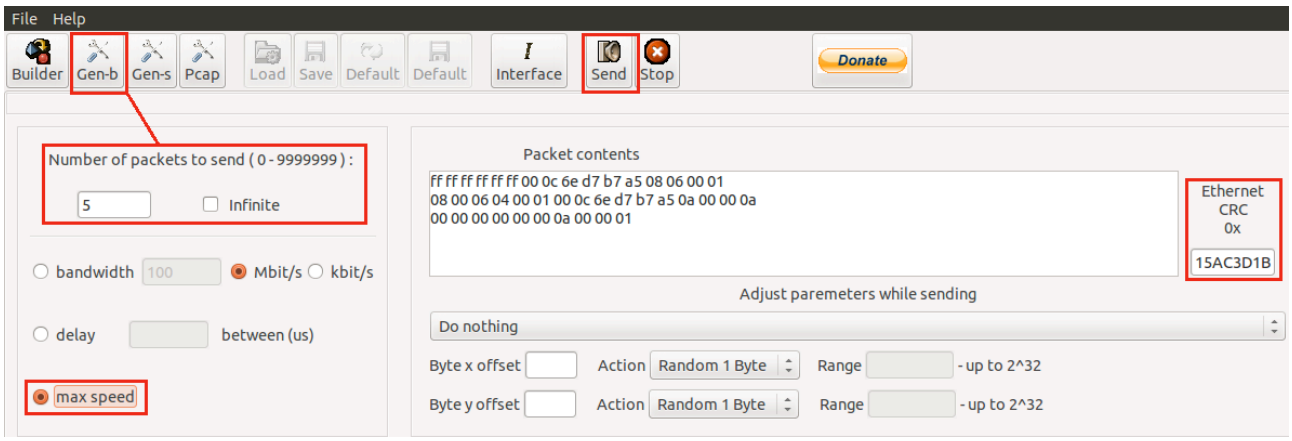

FIGURA 4 Menu *Gen-b* di packETH

Prima di effettuare l'invio vero e proprio apriamo Wireshark (**sudo wireshark**), inseriamo un filtro che visualizza solo il protocollo **arp** e facciamo partire l'analisi cliccando su *Start*.
Torniamo a packETH e clicchiamo su **Send** per inviare i frame sulla LAN.
In FIGURA 5 si mostrano i frame Ethernet creati, catturati con Wireshark, che trasportano le PDU del protocollo ARP.

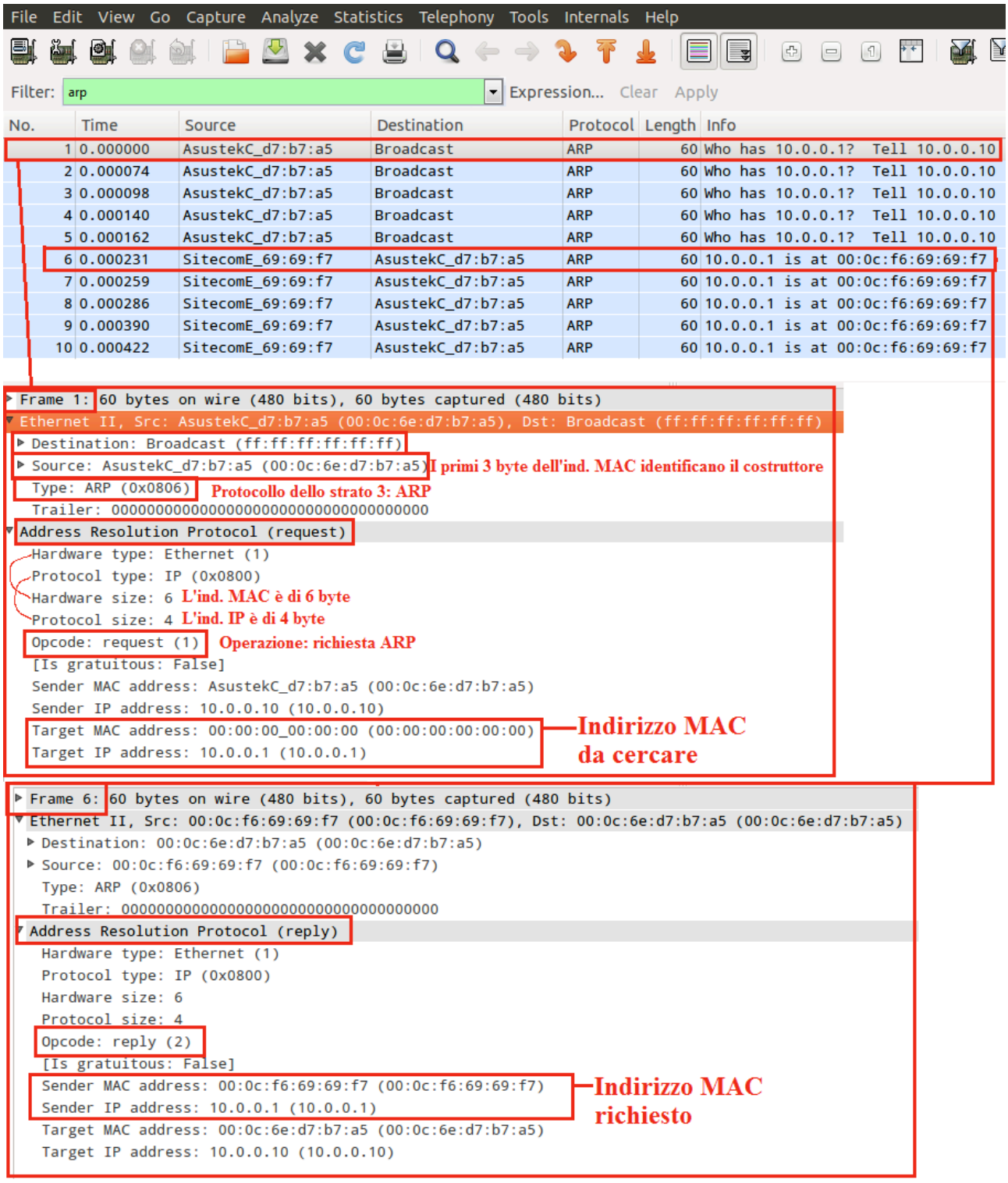

FIGURA 5 Frame Ethernet II che trasportano: Frame 1 -> richiesta ARP (Request); Frame 6 -> risposta ARP (Replay), contente l'indirizzo MAC cercato.

Simulazione con Cisco Packet Tracer
Il laboratorio didattico può anche essere effettuato tramite una simulazione al computer effettuata con il pacchetto software di simulazione **Cisco Packet Tracer**.

Disegniamo la rete di FIGURA 6, assegnando anche gli indirizzi IP.
Inseriamo gli apparati selezionando:
- End Devices, Generic PC-PT per inserire due PC; li rinominiamo come PC9 e PC10 cliccandoci sopra e selezionando **Config**;
- Switches ed inseriamo uno switch 2960;
- Routers ed inseriamo un Router 1941.

Clicchiamo su Connections, Copper Straight-Through e colleghiamo con un cavo Ethernet dritto (Copper Straight-Through):
- le porte FastEthernet dei PC con le porte FastEthernet dello Switch
- la porta GigabitEthernet0/0 del Router con la porta GigabitEthernet dello switch.

Configuriamo ora la porta GigabitEthernet del router assegnandole l'indirizzo IP 10.0.0.1 con subnet mask 255.255.255.0: clicchiamo sul Router, selezioniamo **Config, GigabitEthernet0/0** assegniamo l'indirizzo IP e la subnet mask; selezioniamo infine **On** per abilitare la porta (FIGURA 6). Nella parte bassa della FIGURA 6 sono mostrati i comandi IOS che vengono inviati al router per configurare la sua interfaccia.
Configuriamo anche i PC assegnando loro gli indirizzi IP 10.0.0.9 e 10.0.0.10, cliccandoci sopra, selezionando **Config, FastEthernet** e inserendo l'indirizzo IP e la subnet mask.

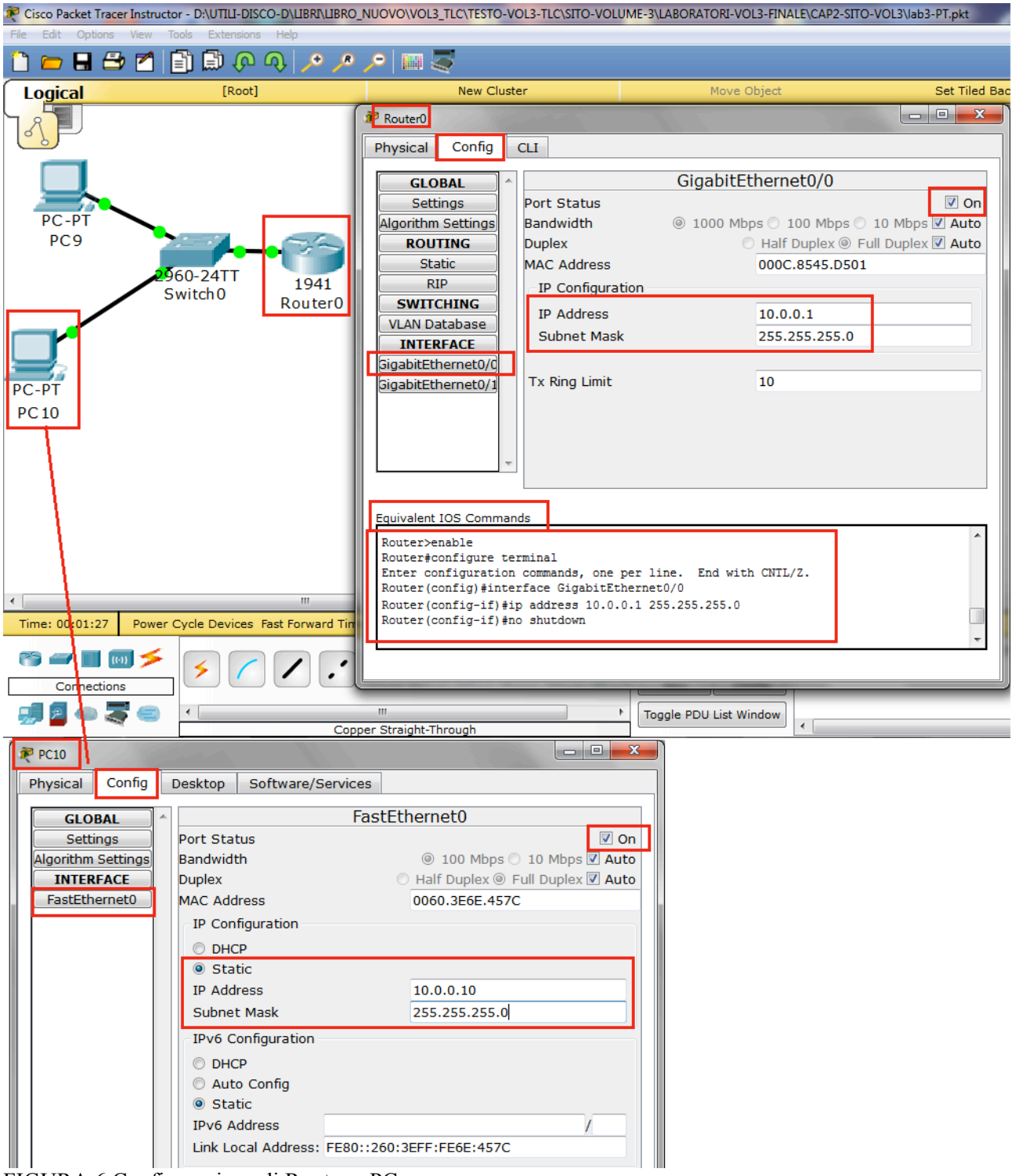

FIGURA 6 Configurazione di Router e PC

Clicchiamo sul PC con indirizzo IP 10.0.0.10 e selezioniamo **Desktop -> Command Prompt**. Passiamo in modalità **Simulation** e inseriamo un filtro che visualizzi solo il protocollo ARP (FIGURA 7); ritorniamo al prompt dei comandi e digitiamo il comando ping 10.0.0.1; clicchiamo quindi su **Play** per vedere il flusso dei pacchetti ARP (FIGURA 8).

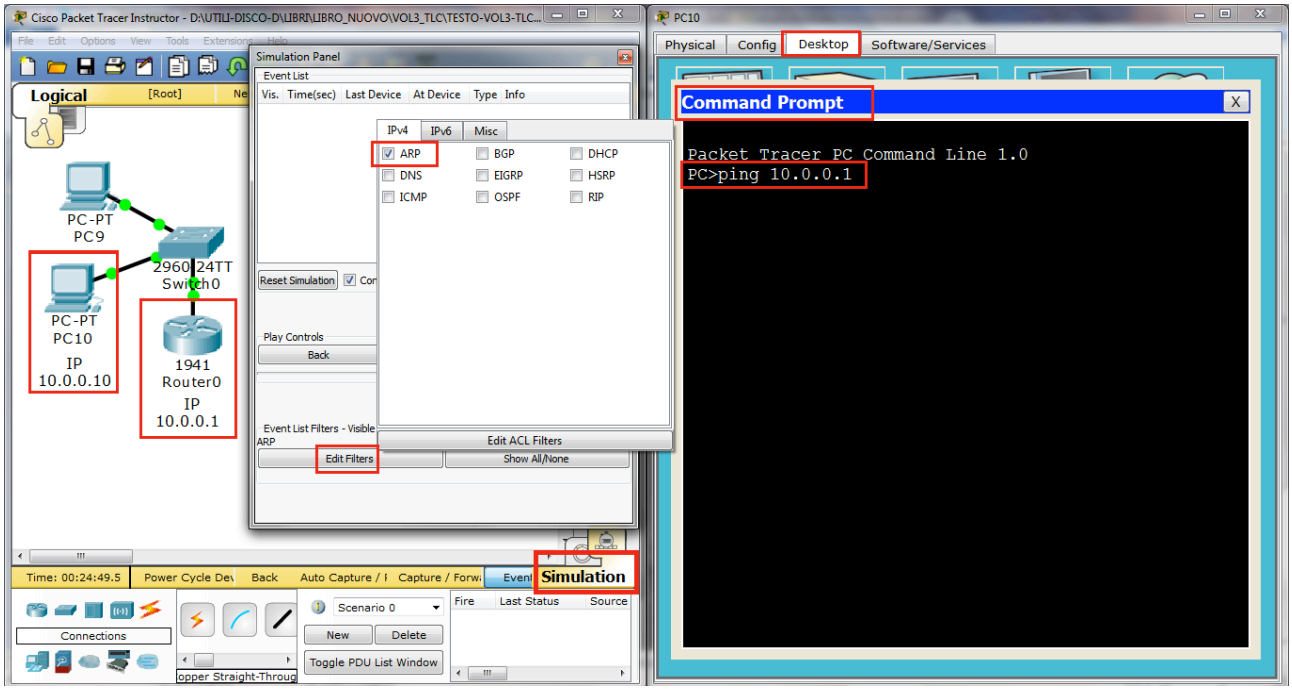

FIGURA 7 Inserimento del filtro in modalità Simulation e Command Prompt del PC10

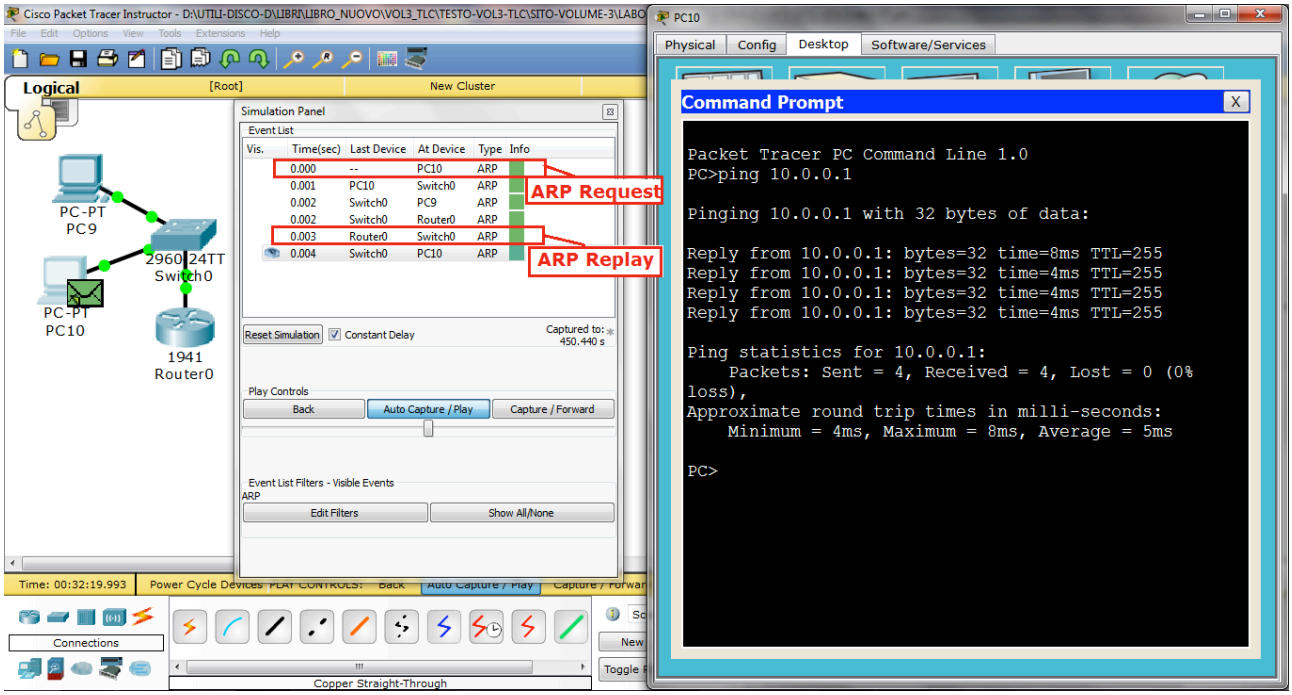

FIGURA 8 Simulazione del flusso di pacchetti ARP e risposte inviate al PC10

Al termine della simulazione clicchiamo dapprima sul pacchetto ARP di *Request* e poi su quello di *Replay* per analizzarne la composizione (FIGURA 9).

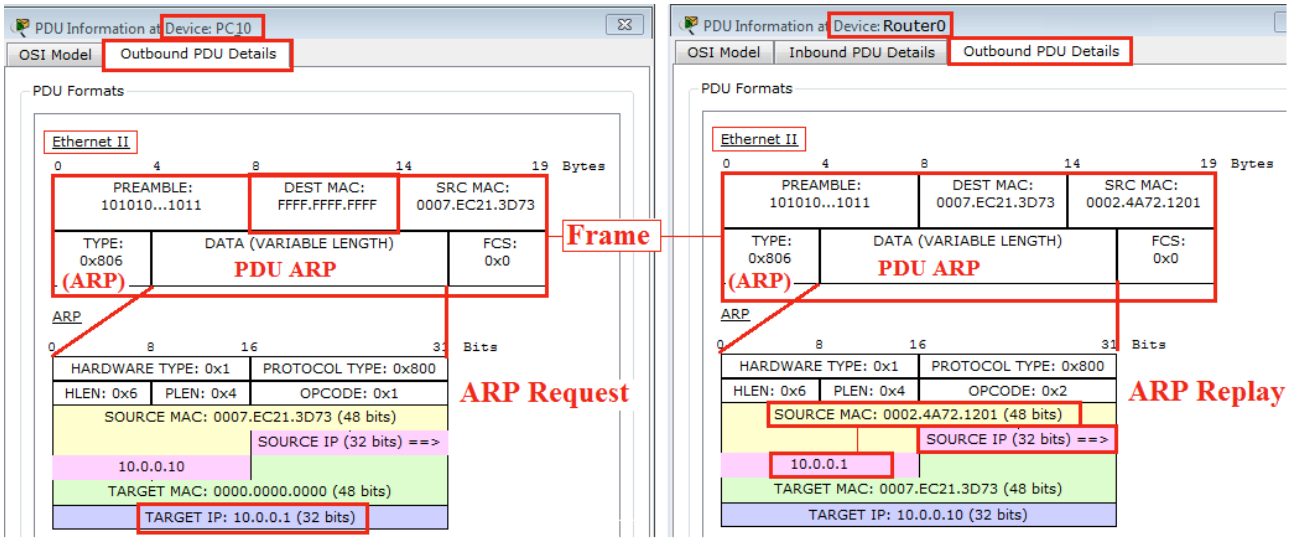

FIGURA 9 Composizione delle PDU (pacchetti) ARP di Request e Replay.