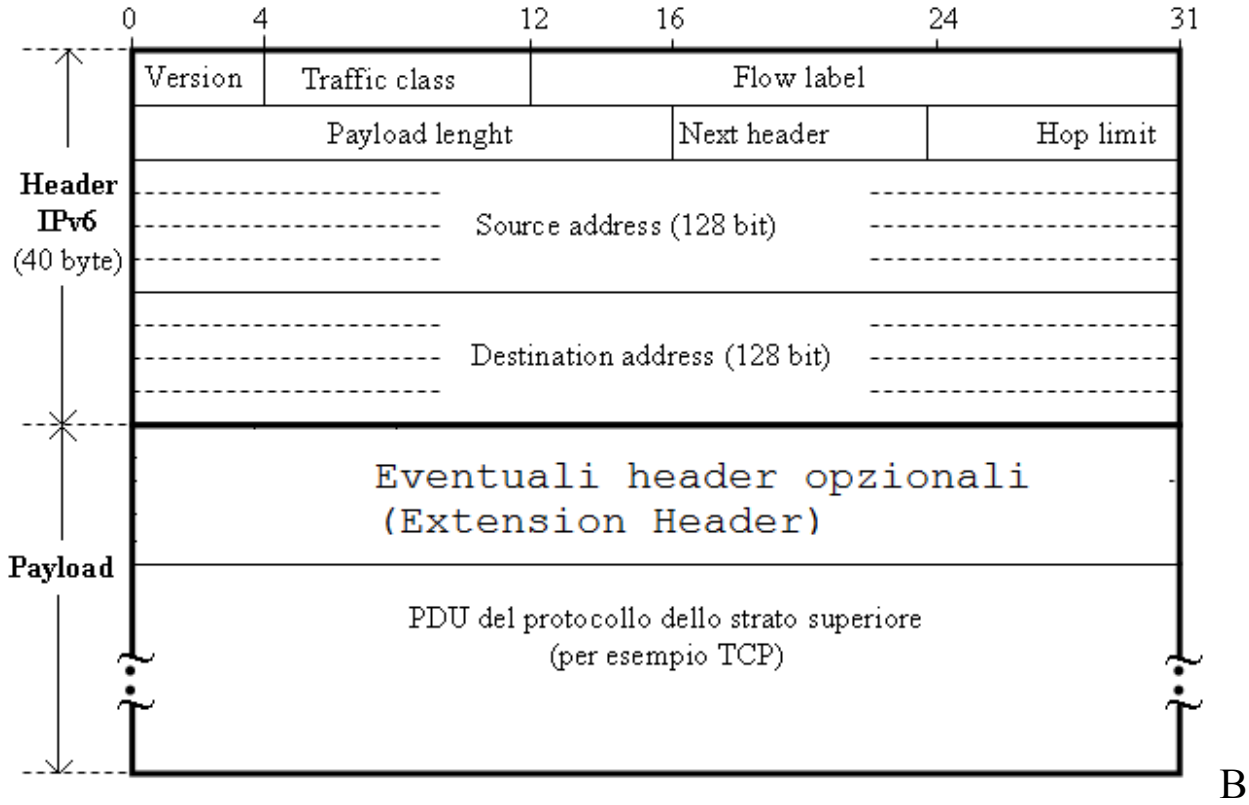
LABORATORIO DIDATTICO 7

Analisi del formato di un pacchetto IPv6 e impiego di ICMPv6 al posto di ARP

In questo LABORATORIO DIDATTICO si propone l'effettuazione dell'analisi del formato di un pacchetto IPv6 con l'analizzatore di protocollo Wireshark.
Operiamo nel seguente modo.

1. Apriamo *Wireshark* su un PC, lo avviamo e inseriamo il Display Filter <*icmpv6*>;
2. Effettuiamo un *ping* con protocollo IMCPv6 dal PC con Wireshark verso un altro PC della stessa LAN, come indicato nel LABORATORIO DIDATTICO 6; per semplificare l'analisi possiamo far inviare dal protocollo IMCPv6 una sola PDU di Echo request, a cui il PC destinazione risponderà con una PDU di Echo replay con il comando <**ping -6 -n 1 indirizzo_IPv6%ZoneID**> (nell'esempio <ping -6 -n 1 fe80::20c:6eff:fed7:b7a5%11>)
3. Fermiamo Wireshark e analizziamo i frame scambiati che trasportano le PDU ICMPv6.

A



B

FIGURA 1 Formato di un pacchetto IPv6: A) tramite un'analisi reale; B) rappresentazione teorica.

Come evidenziato in FIGURA 1, un pacchetto IPv6 è composto da un Header IPv6 (di 40 byte) e da un campo indicato come *payload* (o *data*) che trasporta una PDU (*Protocol Data Unit*) di un protocollo che fa uso di IPv6, in questo caso l'ICMPv6. A sua volta il pacchetto IPv6 viene incapsulato nel campo informativo (payload o data) di un frame Ethernet prima di effettuarne l'invio sul mezzo trasmissivo della LAN.
In FIGURA 1 sono evidenziati i campi che compongono l'header IPv6, che sono i seguenti:

- *Version*, 4 bit; indica la versione del protocollo IPv4 (*Version=6*);
- *Traffic Class* (o *Priority*), 8 bit; identifica la classe di traffico a cui appartiene il pacchetto IPv6; ha una funzione analoga al campo *ToS (Type of Service)* di IPv4; utilizzando questo campo una sorgente può marcare il pacchetto IPv6 come appartenente a una data classe di traffico, avente una certa priorità, e i router possono implementare code di attesa diverse in modo da trattare con priorità differente i pacchetti IPv6 a seconda della classe di traffico di appartenenza;
- *Flow label*, 20 bit; è un campo che consente di etichettare i pacchetti come appartenenti a uno stesso flusso; con il termine *flow* (flusso) si intende una sequenza di pacchetti inviati da una certa sorgente a

una destinazione e per la quale la sorgente richiede un trattamento[1] particolare da parte dei router che vengono attraversati; gli host che non utilizzano questo campo lo pongono a zero, mentre i router che non lo supportano ignorano il suo contenuto;
- *Payload length*, 16 bit; indica la lunghezza in ottetti (byte) della parte di pacchetto che segue l'header IPv6, cioè del *payload*; poiché l'header IPv6 ha lunghezza pari a 40 ottetti, la lunghezza totale di un pacchetto IPv6 è pari alla lunghezza del payload + 40 [ottetti];
- *Next header*, 8 bit; indica il protocollo dello strato superiore (*upper layer*) che utilizza l'IPv6 per trasportare le proprie PDU (Protocol Data Unit); è simile al campo *Protocol* di IPv4, anche nella codifica (6=TCP; 17=UDP, 58=ICMPv6, ecc.); se, invece, sono presenti degli header opzionali, detti *extension heade*r, indica il tipo di header che segue l'header principale IPv6;
- *Hop limit*, 8 bit; il numero contenuto in questo campo viene decrementato di 1 da ogni nodo (router) che inoltra il pacchetto; se l'Hop limit raggiunge il valore "0" il pacchetto viene scartato; equivale al campo TTL (*Time To Live*) di IPv4 e in pratica indica il numero di router (o hop, salti) che il pacchetto può ancora attraversare;
- *Source address*, 128 bit; indirizzo IPv6 dell'host sorgente, che emette il pacchetto;
- *Destination address*, 128 bit; indirizzo IPv6 della destinazione[2].

La formazione di un pacchetto IPv6 può anche essere studiata impiegando il pacchetto software packETH. Dopo aver rilevato gli indirizzi IPv6 ed averli aggiunti all'Address database di packETH, si può operare nel seguente modo (FIGURA 2):

1. si compilano i campi dell'header MAC (protocollo Ethernet) selezionando: gli indirizzi MAC della scheda di destinazione e di quella sorgente (cliccando su Select si apre l'Address Database); il protocollo dello strato 3 IPv6 (Ethertype);
2. Si compilano i campi vuoti dell'header IPv6 (Next layer -> IPv6), selezionando: l'indirizzo IPv6 dell'host sorgente e di quello di destinazione (dall'Address database); si seleziona quindi come Next layer ICMPv6 (la cui codifica in esadecimale, 0x3A corrispondente a 58 in decimale viene inserita automaticamente nel campo Next Header;
3. Si compilano i campi dell'header ICMPv6 inserendo: il tipo di messaggio (Type 0x80 per l'Echo request), il codice (Code 0x00), si seleziona Data e come Data pattern mettiamo per esempio 00, con lunghezza 32 byte;
4. Si seleziona l'interfaccia di uscita (Interface eth0), si clicca su Gen-b e si specifica il numero di pacchetti da inviare, per esempio 2, e la banda (velocità); si clicca infine su Send per inviare i pacchetti (rilevabili con Wireshark).

[1] Il tipo di trattamento che si richiede può essere definito nell'*extension header Hop-by-Hop Options* o in altro modo; combinando la classe di traffico e l'etichettatura dei flussi di pacchetti è possibile implementare livelli di QoS (*Quality of Service*) diversi e adattabili a esigenze specifiche degli utenti, consentendo così sia di personalizzare i servizi sia di supportare applicazioni multimediali (che combinano audio, video e dati).

[2] Con IPv6 può anche non essere l'indirizzo dell'host di destinazione finale del pacchetto, se è presente un header opzionale di routing (*routing header*) che consente di effettuare degli ulteriori instradamenti per tenere conto, ad esempio, della mobilità di un terminale; il *destination address* può contenere l'indirizzo di un *router* di destinazione, il quale esaminando l'header di routing opzionale determina quale ulteriore instradamento va effettuato per raggiungere l'host di destinazione effettivo.

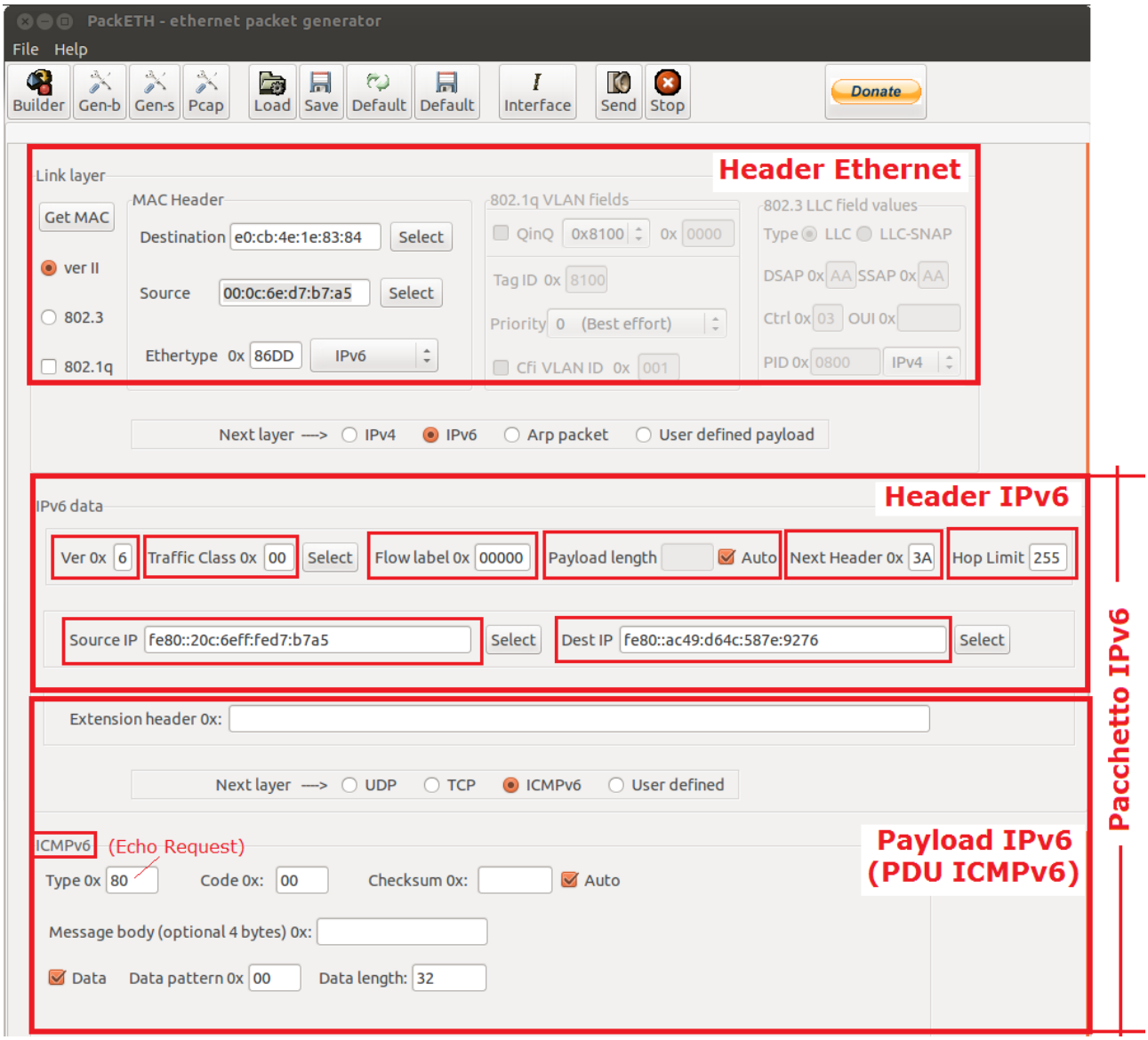


FIGURA 2 Creazione di un pacchetto IPv6 con packETH.

Extension Header IPv6

Gli *extension header* trasportano informazioni di servizio opzionali che vengono elaborate dal nodo specificato dall'indirizzo di destinazione; fa eccezione l'header opzionale *Hop-by-Hop Options header* che viene analizzato anche dai router intermedi, in quanto può trasportare informazioni relative a come essi devono trattare un pacchetto IPv6. Le funzioni principali degli header opzionali sono le seguenti:

- *Hop-by-Hop Options header*; viene utilizzato per trasportare informazioni opzionali che devono essere esaminate da ogni router attraversato dal pacchetto, per esempio questo campo viene utilizzato quando si desidera trasmettere un pacchetto IPv6 avente un payload di dimensioni maggiori di 2^{16}=65536 ottetti (dimensione massima consentita dal campo *payload lenght* dell'header IPv6), denominato *jumbo payload*; le reali dimensioni del payload vengono specificate in questo campo; inoltre le opzioni contenute in questo campo potrebbero indicare ai router come trattare il pacchetto in relazione alla flow label che lo contraddistingue, in modo da soddisfare i parametri di qualità del servizio (QoS) concordati con l'utente per quel determinato flusso di pacchetti;
- *Routing header*; può essere utilizzato da una sorgente per allegare al pacchetto l'elenco degli indirizzi di uno o più router da attraversare lungo il percorso che porta all'effettivo nodo di destinazione; se utilizza questa opzione la sorgente immette come indirizzo IPv6 di destinazione nell'header principale l'indirizzo di un router e inserisce nel *routing header* l'elenco degli indirizzi IPv6 dei router a cui deve essere ulteriormente inoltrato il pacchetto, seguiti, in ultima posizione, dall'indirizzo IPv6 dell'effettivo host di destinazione; in questo modo il pacchetto viene recapitato al router indicato nell'header principale, il quale esamina il *routing header*, aggiorna l'indirizzo di destinazione del pacchetto inserendovi il primo indirizzo

elencato, eliminandolo dalle opzioni, e inoltra il pacchetto; in questo modo si raggiunge il primo router specificato nelle opzioni, che ripete le stesse operazioni; il pacchetto viene così inoltrato verso l'effettivo host di destinazione dai router specificati nell'elenco;

- *Fragment header*, viene utilizzato da una sorgente per frammentare un pacchetto di dimensioni maggiori del *path MTU* (*Maximum Transmission Unit* utilizzabile sull'intero percorso); il pacchetto originario viene riassemblato dal nodo di destinazione; i campi contenuti in questo header sono analoghi a quelli che consentono la frammentazione dei pacchetti IPv4; al contrario di IPv4, però, la frammentazione dei pacchetti IPv6 può essere effettuata solamente dalla sorgente e non dai router intermedi; i nodi IPv6 sorgente devono così implementare un algoritmo che consenta loro di scoprire qual è il *path MTU* verso una data destinazione, in modo da determinare se il pacchetto va frammentato o meno; in caso contrario la dimensione del pacchetto va limitata a 1280 ottetti, che assicura il trasporto di un pacchetto IPv6 senza frammentazione in quanto è il valore minimo di MTU richiesto da IPv6 a un qualsiasi link;
- *Authentication header*; consente l'autenticazione del pacchetto IPv6, in modo da essere sicuri che il pacchetto sia stato realmente inviato dal nodo specificato dall'indirizzo sorgente e che non abbia subito alterazioni lungo il percorso verso la destinazione;
- *Encapsulating Security Payload header*; consente di crittografare i messaggi trasportati dai pacchetti IPv6 in modo da tutelare la privacy; utilizzando meccanismi di autenticazione e crittografia si realizza una architettura di sicurezza per l'IPv4 (*IPsec, Internet Protocol security architecture*, si veda l'Unità 13) in grado di proteggere le comunicazioni su Internet;
- *Destination Options header*; viene utilizzato per trasportare informazioni opzionali che vanno esaminate dal nodo identificato dall'indirizzo di destinazione dell'header IPv6; se questo campo precede il *routing header*, le opzioni in esso contenute sono esaminate anche dai nodi specificati nel *routing header*, mentre se viene collocato come ultimo *extension header*, le opzioni sono esaminate solo dall'host di destinazione finale.

Tranne il *fragment header*, che è di lunghezza fissa, gli *extension header* sono di lunghezza variabile, per cui al loro interno sono presenti due campi: *next header*, per indicare il tipo di header che segue, e *header lenght*, per specificare la lunghezza di ciascun *extension header* (fa eccezione l'Encapsulating Security Payload). In TABELLA 5 sono riportati i principali codici (in formato decimale) che possono essere contenuto nel campo *next header*, sia dell'header IPv6 sia degli *extension header*.

TABELLA 5 Principali valori contenuti nel campo *Next header* e loro significato

Codice	**Significato**
6	Segue l'header *TCP*
17	Segue l'header *UDP*
58	Segue l'header *ICMPv6*
0	Segue l'extension header *Hop-by-Hop Options*
43	Segue l'extension header *Routing*
44	Segue l'extension header *Fragment*
50	Segue l'extension header *Encapsulation Security Payload*
51	Segue l'extension header *Authentication*
59	*no next header* (non segue alcun header)
60	Segue l'extension header *Destination Options*

Uso di ICMPv6 in sostituzione del protocollo ARP

Con il protocollo IPv6 scompare il protocollo ARP, che viene sostituito con i messaggi del protocollo **ICMPv6 Neighbor Solicitation** e **Neighbor Advertisement**.
Per esempio prima di effettuare un ping l'host sorgente deve ricercare l'indirizzo MAC dell'host destinazione (o target). Con IPv6 ciò avviene nel seguente modo:

- con il messaggio **ICMPv6 Neighbor Solicitation** (avente come Type 135) un host (Source) richiede l'indirizzo MAC, o *Link-Layer address*, di un host (Target) di cui conosce l'indirizzo IPv6, inviando la richiesta in multicast (multicast IPv6), FIGURA 3;
- l'host target risponde con un messaggio **ICMPv6 Neighbor Advertisement** (avente come Type 136), in cui inserisce il proprio indirizzo MAC (Link-Layer address), FIGURA 4.

Solo dopo vengono inviati i messaggio ICMPv6 di Echo Request ed Echo Replay legati al ping.

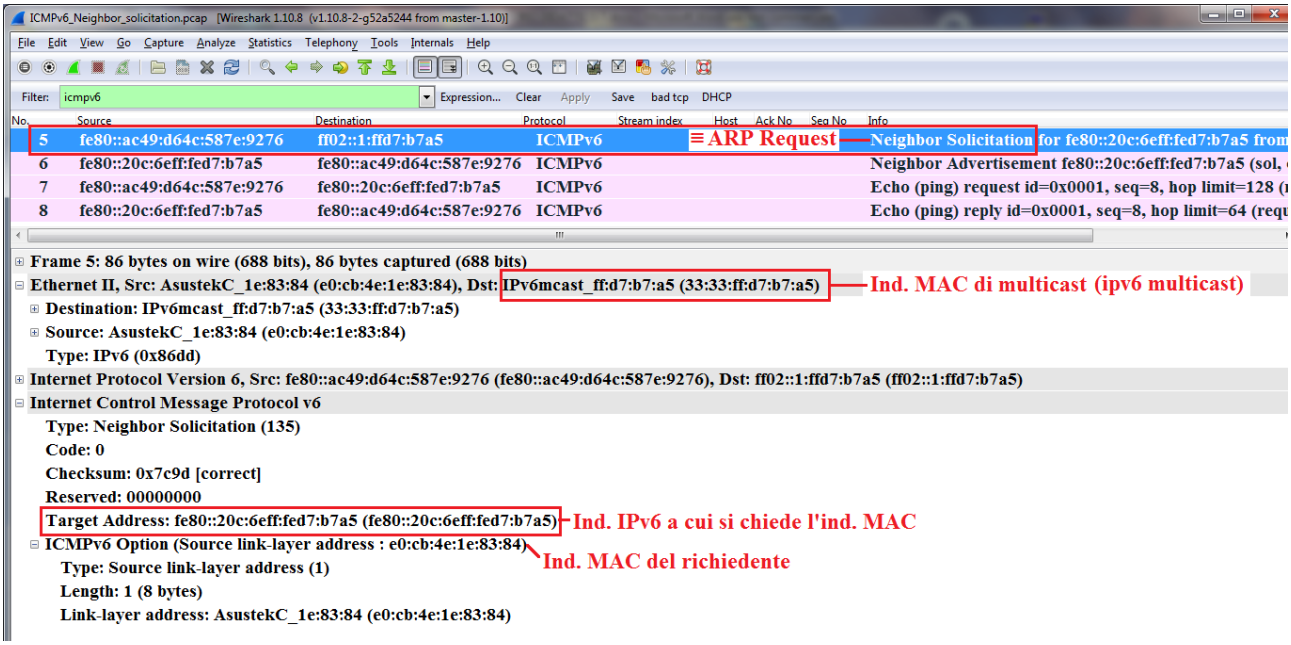


FIGURA 3 Richiesta di un indirizzo MAC con un messaggio ICMPv6 Neighbor Solicitation

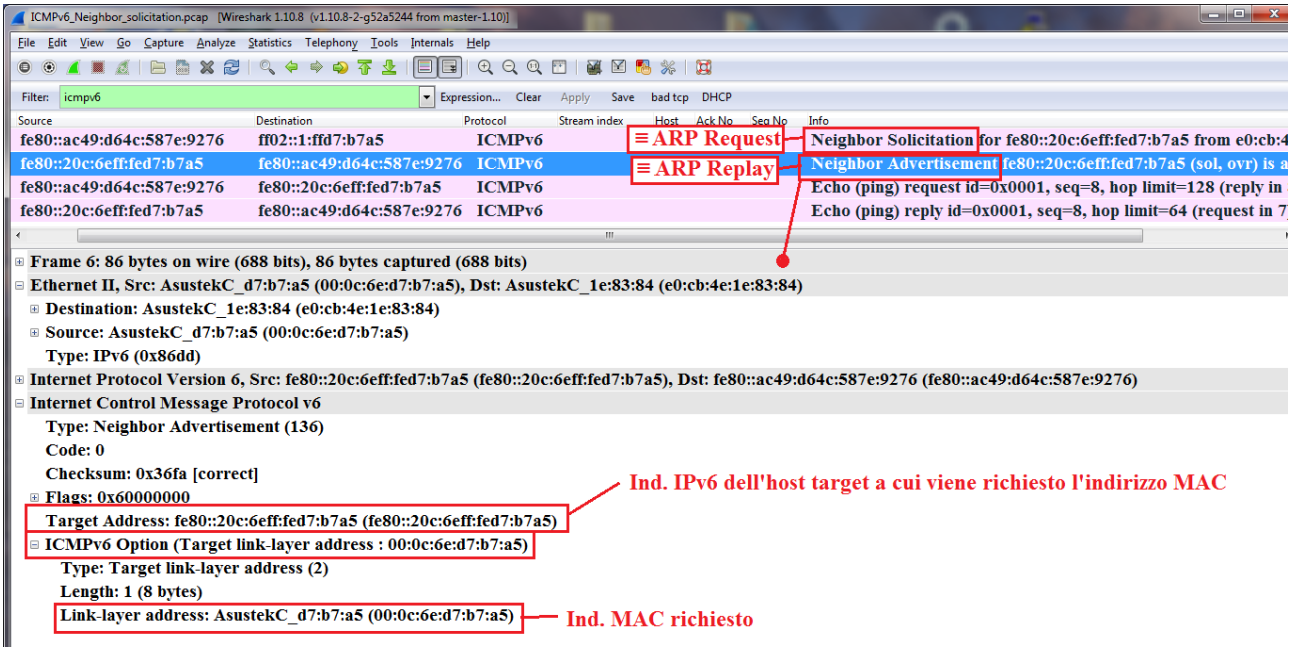


FIGURA 4 Risposta dell'host target con invio del proprio indirizzo MAC in un messaggio ICMPv6 Neighbor Advertisement