Sicurezza e IPv6

Il buono, il brutto e il cattivo del nuovo protocollo di comunicazione IP

Stefano Maccaglia
Matteo Dominizi

Special thanks to: Federico Lustrissimi & Marco Scordino

Intro: Il tradizionale modello ISO/OSI

- Non possiamo dedicarci alle comunicazioni di rete senza aver prima osservato un minuto di attenzione al modello ISO/OSI: la famosa «pila» di protocolli suddivisa in 7 livelli (Layer), che insieme espletano in maniera logico-gerarchica tutte le funzionalità della rete.
- I ***layer*** racchiudono uno o più aspetti fra loro correlati della comunicazione fra due nodi di una rete. I layer sono in totale 7 e vanno dal livello fisico (quello del mezzo fisico, ossia del cavo o delle onde radio) fino al livello delle applicazioni, attraverso cui si realizza la comunicazione di *alto livello*

Intro: alcuni aspetti del «passaggio»

- L'IPv6 e l'IPv4 hanno molti aspetti in comune
  - I meccanismi base di funzionamento sono gli stessi
  - Il layer applicativo non è stato impattato
  - La Sicurezza del Protocollo IPv6 dovrebbe assicurare una maggiore protezione, *ma ancora non è così*
  - L'IPv6 introduce nativamente il supporto all'IPSec, ma non è ancora stato adottato
  - L'IPv6 non integra meccanismi di protezione maggiori per i layer superiori.

Novità introdotte da IPv6

- Alcuni contenuti del pacchetto IPv4 sono stati rimossi:
  - **Non c'è più il broadcast address**
  - Non è più possibile utilizzare le opzioni di traceroute per identificare delle path filtrate
  - Non c'è più il campo «IP ID» nell'header
    - Il che impedisce di calcolare il tempo di uptime di un Sistema
  - Non c'è più il campo opzionale IP Record Route
  - **Il Multicast non può essere attivato da remoto**
- **Tutto questo comporta l'impossibilità materiale di scansionare gli host attivi in rete attraverso il tradizionale PING al Broadcast address.**

Novità introdotte da IPv6

- Ma al pari nuove opportunità per la scansione massiva degli host attivi possono nascere dall'adozione del multicast, almeno nell'identificazione dei server nella rete locale (Routers, NTP Server, ecc...)
- In effetti gli indirizzi multicast locali permettono ad un host IPv6, regolarmente, di identificare gli altri host nella propria subnet.
- Questo permette l'adozione di tecniche di scansione, in rete locale, addirittura più raffinate di quanto si possa oggi realizzare in IPv4.
- Da remoto le cose invece si fanno più complicate in quanto gli host di una rete possono facilmente impedire il Ping Scan.

IPv6 Protocol Header

- **L'header IPv6 non presenta vulnerabilità**:
  - Il problema nasce da come questi pacchetti vengono creati ed elaborati.
- **La grandezza dell'header IPv6 è fissa**:
  - Dimensioni proporzionalmente inferiori rispetto all'header IPv4;
  - La maggior parte delle funzionalità opzionali sono state trasferite nei flessibili extension header.
- I campi dell'header possono essere utilizzati per poter effettuare delle **comunicazioni nascoste**:
  - Inserendo informazioni nei vari campi, come avviene per l'IPv4;
  - Sfruttando l'elasticità operazionale degli extension header.

L'Header IPv6

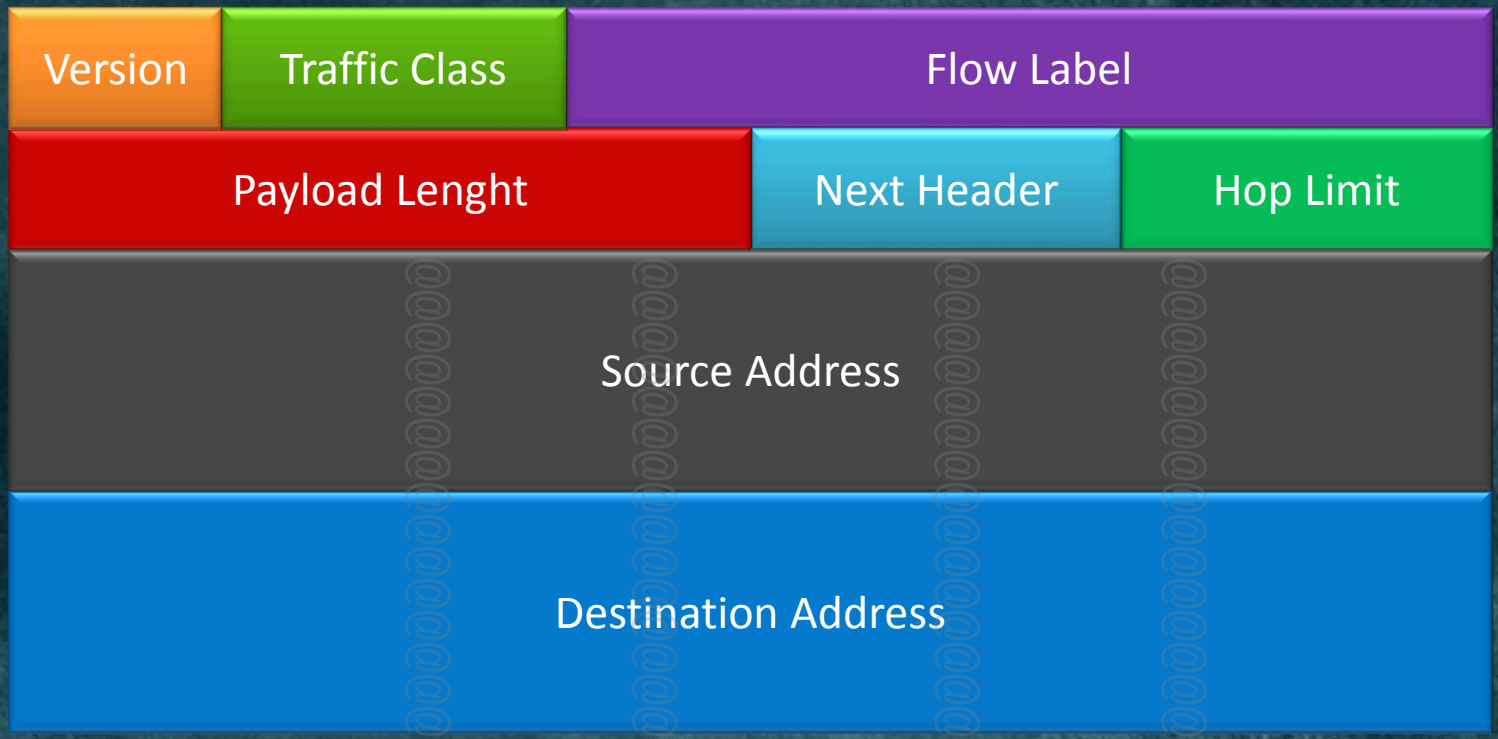
Nonostante l'indirizzo IPv6 è quattro volte più grande rispetto a quello IPv4 (32bit vs 128bit), il nuovo header è più piccolo rispetto a quello del suo predecessore.

Questo grazie all'**ottimizzazione** dei campi presenti:

- Eliminazione di campi superflui;
- Aggiunta degli Extension Header in cui inserire le informazioni non sempre necessarie.

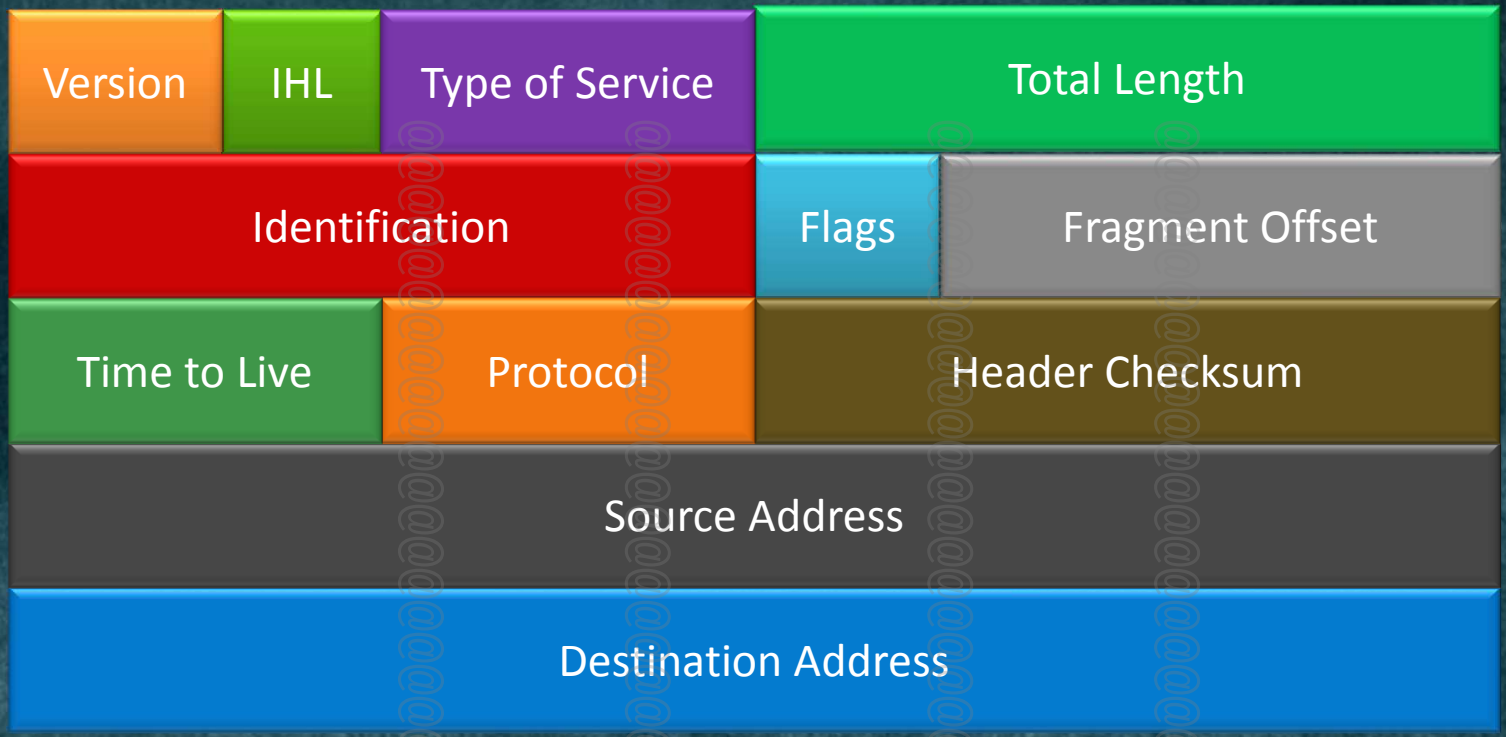
Questo ha permesso una maggiore **efficienza** in termini di **funzionalità** e di **forwarding**, introducendo però una flessibilità dai risvolti positivi quanto negativi.

Header IPv6

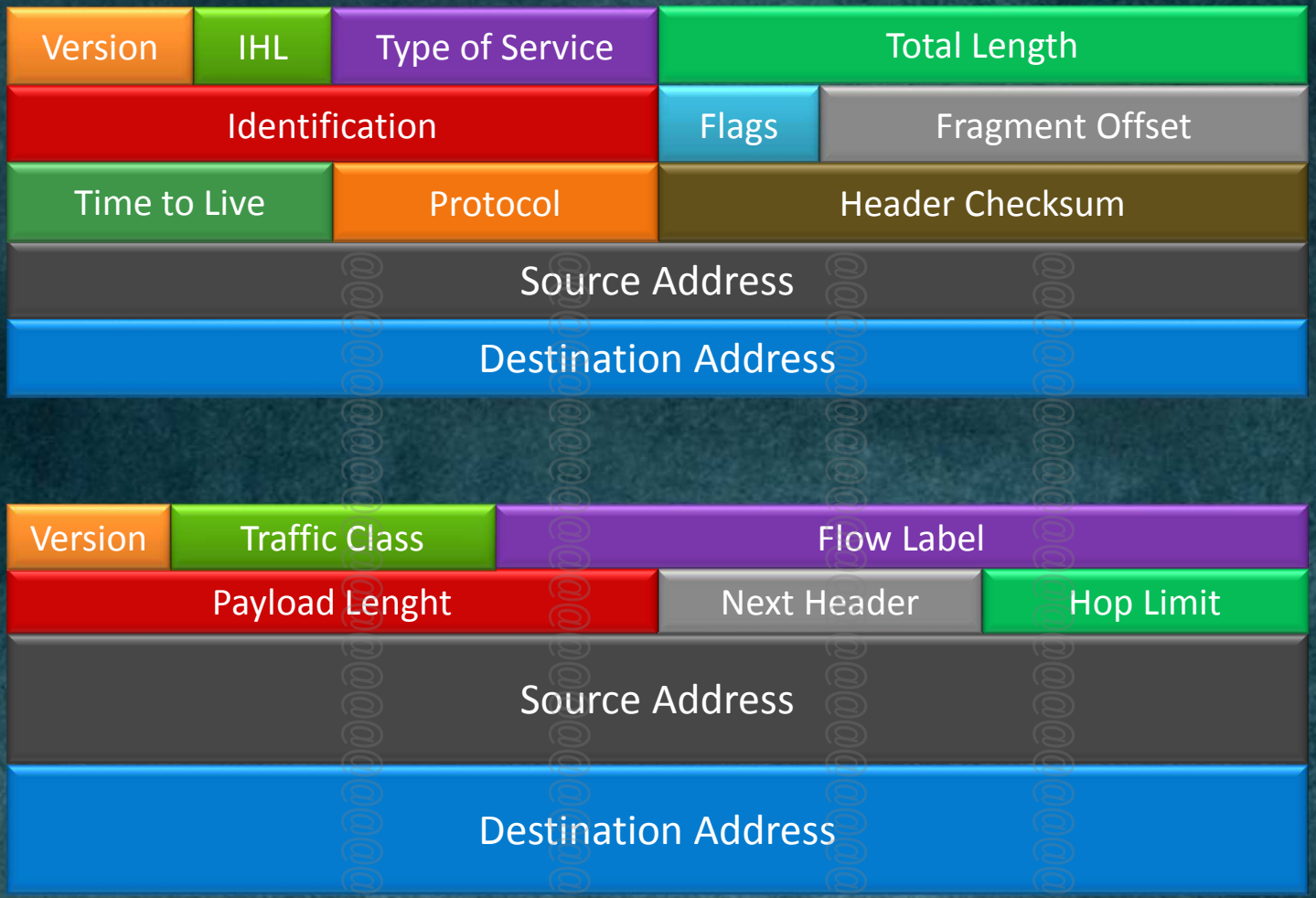


Anche in questo contesto c'è ovviamente il rischio di trovare delle comunicazioni nascoste all'interno dei campi dell'header nonostante le dimensioni limitate.

Header IPv4


Version
IHL
Type of Service
Total Length
Identification
Flags
Fragment Offset
Time to Live
Protocol
Header Checksum
Source Address
Destination Address

Differenze header IPv4-IPv6



Sicurezza nel nuovo formato degli indirizzi

Il **live scanning** è una delle tecniche di riconoscimento più utilizzata in IPv4.

I "Blackhats" con i live scanning possono effettuare una **discovery** di tutte le macchine attive all'interno di una sottorete locale.

Un indirizzo di classe C in IPv4 utilizza 8 bit per l'host addressing:

$$2^8 host * \frac{1\ sec}{1\ host} * \frac{1\ min}{60\ sec} = 4.267\ min$$

Mentre una subnet IPv6 ne utilizza 64 bit:

$$2^{64} host * \frac{1\ sec}{1\ host} * \frac{1\ year}{31{,}536{,}000\ sec} = 584{,}942{,}417{,}355\ years$$

ICMPv6 come fondamento delle comunicazioni

Nell'IPv6 l'ICMP riveste un ruolo fondamentale, in quanto non solo costituisce un potentissimo strumento di **autodignostica** ma funge anche da perno fondamentale nel **supporto allo stack di comunicazione**.

Tipologie di messaggi ICMPv6:

- **ICMPv6 d'errore**, per la comunicazione di eventuali problematiche di trasmissione;
- **ICMPv6 d'informazione**, per il corretto funzionamento dei protocolli interessati.

Per queste ragioni il **protocollo ICMPv6** è sicuramente un bersaglio critico, in quanto fulcro di diverse tipologie di attacco molto comuni.

ICMPv6

L'ICMPv6 gioca un **ruolo chiave** nel funzionamento del nuovo protocollo:

- **Non può essere filtrato**, o almeno non del tutto , a differenza di quanto accade per l'IPv4 dove l'ICMP non è essenziale, tanto che lo si preferisce bloccare in quanto fonte di diversi tipi di attacchi;

- Ovviamente non tutti i type di messaggio ICMPv6 sono indispensabili, è fondamentale studiarne le caratteristiche di utilizzo per limitarne l'utilizzo solo ove necessario.

Blocco composizione ICMPv6

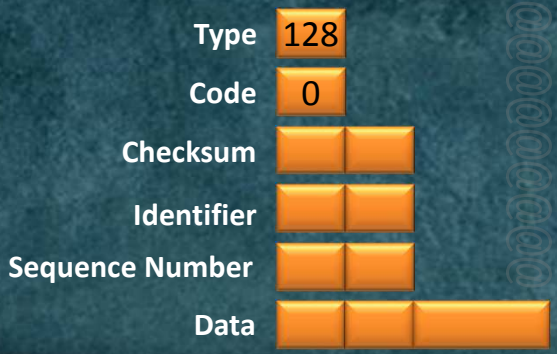
Stabilisce il formato del resto del messaggio ICMP

Dipende dal tipo di messaggio ICMP e permette una più puntuale indicazione di parametri operativi in alcuni casi

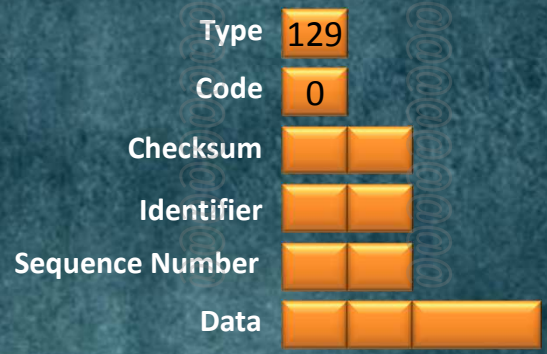
E' usato per verificare la congruità dell'header ICMPv6 e dell'header IPv6

Dipende dal tipo e dal codice del messaggio

Echo Request



Echo Reply



ICMPv6 – Error Messages

A causa della notevole dimensione dell'MTU IPv6 (1280byte), all'interno del **payload** dei messaggi d'errore è contenuta una parte del messaggio originale, se non tutto il messaggio originale stesso:

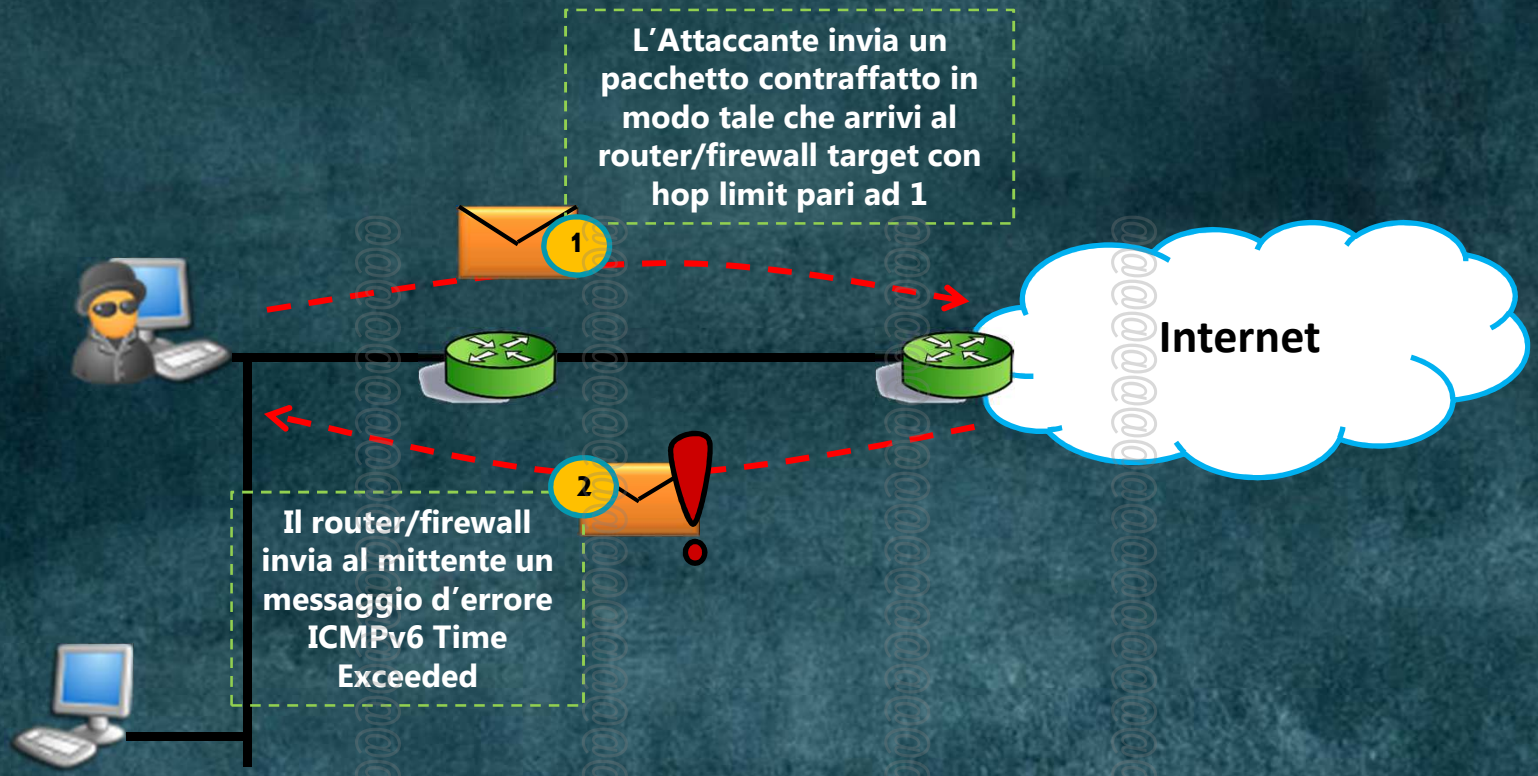
- Tali messaggi possono essere utilizzati come **canali segreti di comunicazione** tra due end-point.

A tale scopo è necessario settare i firewall in modo da controllare la legittimità di tali messaggi, ad esempio controllando che gli **indirizzi di sorgente e destinazione** contenuti nell'header e nel payload del messaggio di errore coincidano.

I messaggi particolarmente critici e soggetti a questo tipo di problematiche sono sicuramente:

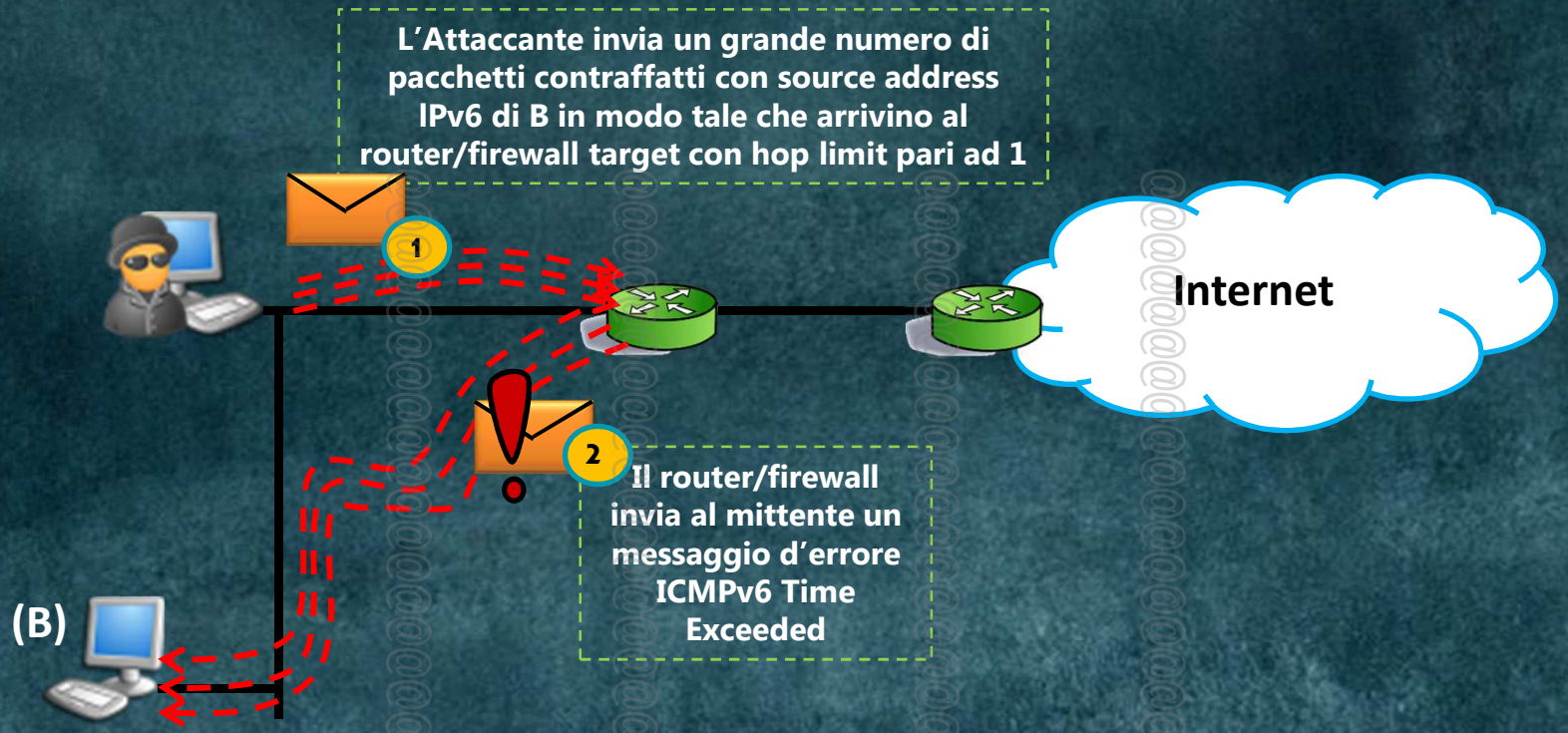
- **Type 1:** Destination Unreachable
- **Type 2:** Packet Too Big—PMTUD
- **Type 3:** Time Exceeded
- **Type 4:** Parameter Problem

Tipico attacco DoS (Time Excedeed)



In questo caso l'attaccante forgia un grande numero di pacchetti per unità di tempo cercando di bloccare il router/firewall.

Tipico attacco DoS (Time Excedeed)



In questo caso l'attaccante forgia un grande numero di pacchetti per unità di tempo cercando di bloccare il target (B).

ICMPv6 attacchi e tecniche di mitigazione

I messaggi ICMPv6 possono essere utilizzati anche solo per acquisire informazioni importanti sulla topologia di rete, fondamentali per apportare l'attacco vero e proprio:

- Tali tipi di attacchi solitamente vengono portati:
  - Ponendosi passivamente in **listening** dei pacchetti IPv6 che transitano;
  - Sfruttando il protocollo per un **testing** attivo della rete.

La prima raccomandazione da seguire quindi è quella di non inviare i tipi di messaggi ICMPv6, che non servono ai fini del protocollo IPv6:

Di seguito i tipi di messaggi ICMPv6 non indispensabili che dovrebbero essere **bloccati**:

- **Unallocated error messages: Type 5–99 and type 102–126**
- **Unallocated informational messages: Type 155–199 and type 202–254**
- **Experimental messages: Type 100, 101, 200, 201**

ICMPv6 – information messages

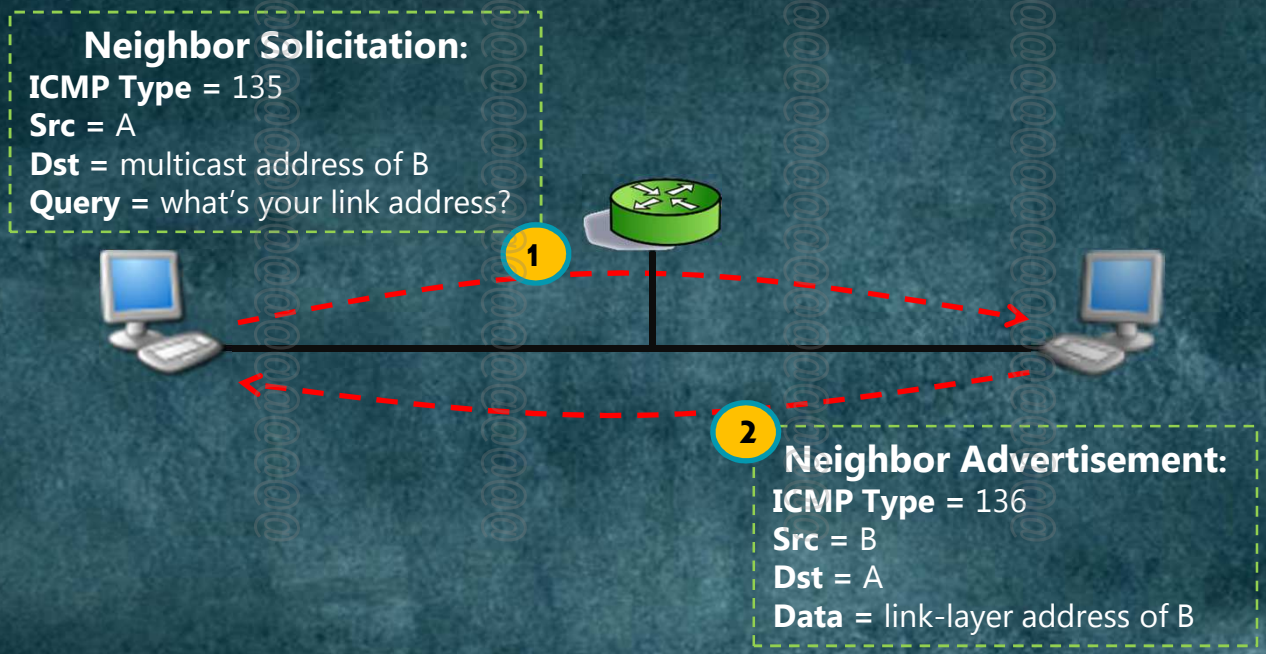
- **Neighbor Discovery Protocol (NDP), Neighbor Advertisements (NA),** e **Neighbor Solicitations (NS)** forniscono l'equivalente funzionalità del protocollo ARP in IPv4:
- **Router Advertisements (RA)** and **Router Solicitations (RS)** aiutano i nodi a determinare informazioni sulla propria LAN (prefisso di rete, default gatway, ecc);
- **Echo Request** and **Echo Reply** supportano l'utilizzo del *ping6;*
- **PMTUD** determina le dimenzioni dell'MTU per la comunicazione;
- **Multicast Listener Discovery (MLD)** fornisce IGMP come funzionalità per comunicazioni multicast;
- **Multicast Router Discovery (MRD)** ricerca router multicast;
- **Node Information Query (NIQ)** condivide informazioni tra nodi;
- **Secure Neighbor Discovery (SEND)** aiuta la sicurezza delle comunicazioni tra neighbor;
- **Mobile IPv6** usato per comunicazioni mobili.

Neighbor Discovery Protocol

È la famiglia di protocolli che combina le funzionalità dell'ARP e del router discovery e redirect del vecchio protocollo IPv4.

I nodi IPv6 utilizzano il Neighbor Discovery per i seguenti obiettivi:

- Determinare gli indirizzi di layer 2 dei nodi sullo stesso link;
- Cercare router nei neighbor che possono forwardare I loro pacchetti;
- Tenere traccia dei neighbor raggiungibili e quelli non raggiungibili, e rilevare le variazioni di indirizzi al link-layer.



Primo Problema: NDP Table

- Le reti contengono:

  2**64 indirizzi, ovvero **18,446,744,073,709,551,616 host**
- I più comuni switch multilayer riescono a trattenere un massimo di NDP entry molto più basso.
- Ad esempio:
  - Juniper EX4200: ≦ 16.000
  - Cisco Nexus 5500: ≦ 6.500
- Anche gli chassis più grandi e potenti riescono a mantenere solo una porzione di record di una potenziale sottorete
- Normalmente tra le 32.000 e le 100.000 Entry

Primo Problema: NDP Table

- Le entry NDP sono necessarie per inoltrare il traffico degli host a livello Accesso.
- Il lavoro dell'NDP è simile a quello dell'ARP per l'IPv4.
- Un potenziale attacco DoS realizzato a danno degli switch di accesso attraverso il flood di Entry NDP può bloccare un'intera rete IPv6.
- D'altro canto gli switch implementano delle feature che possono filtrare questo tipo di attacchi, ma normalmente queste feature non si usano per non pregiudicare il funzionamento della rete IPv6.
- Spesso il problema è anche legato ad un fattore culturale, come vedremo anche per altre casistiche:
  - Gli Amministratori di rete non si sono ancora messi a studiare sul serio l'IPv6…
  - Inoltre, per quanto i produttori promettano futuri miracoli non è pensabile che uno switch di livello Accesso possa trattenere una quantità di record vicina ai valori di una subnet IPv6

Information Disclosure via IPv6?

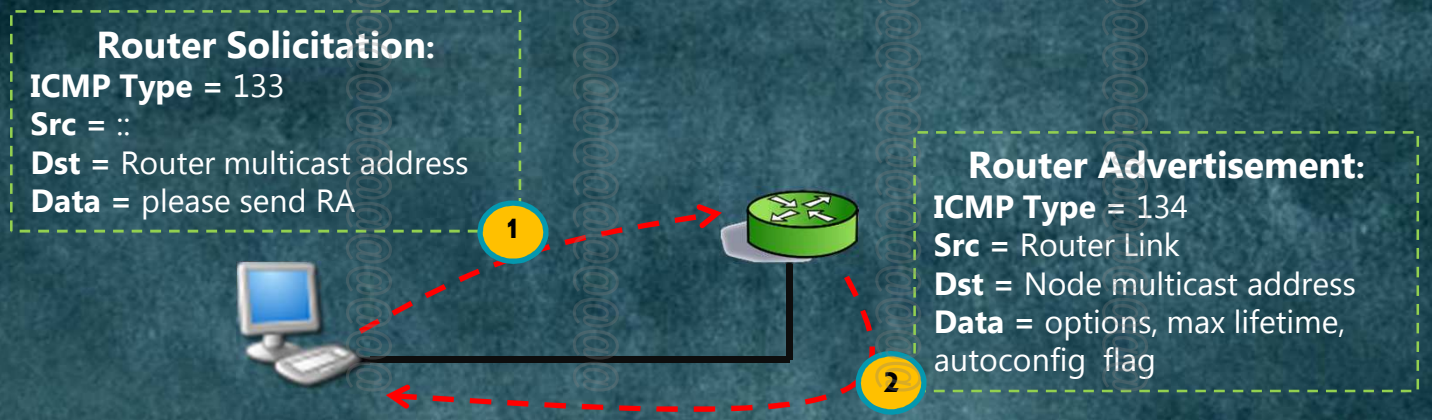
- Già oggi uTorrent, usa il protocollo P2P BitTorrent per permettere la condivisione di musica e video.
- uTorrent è capace, attraverso il meccanismo IPv6/IPv4 chiamato Teredo di nascondere il proprio traffico imbustandolo in IPv6 prima di inviarlo via rete IPv4.
- Anche Vuze, un noto network BitTorrent, permette questo meccanismo di imbustamento IPv6 su IPv4.
- In questo modo l'applicazione BitTorrent crea pacchetti IPv6 contenenti le comunicazioni da realizzare e poi, via Teredo, li imbusta in IPv4 inviandoli nella rete. Quando giungeranno all'end point IPv4 BitTorrent, verranno poi inoltrati a destinazione.

SLAAC

Consiste nella possibilità di ottenere automaticamente un indirizzo IPv6 senza la necessità di effettuare richieste a DHCPv6 Server.

Ogni host completerà il proprio indirizzo IPv6 aggiungendo al prefix ricevuto dal gateway il proprio indirizzo MAC:

- Sfrutta le funzionalità dell'ICMPv6
  - Router Advertisement;
  - Router Solicitation.

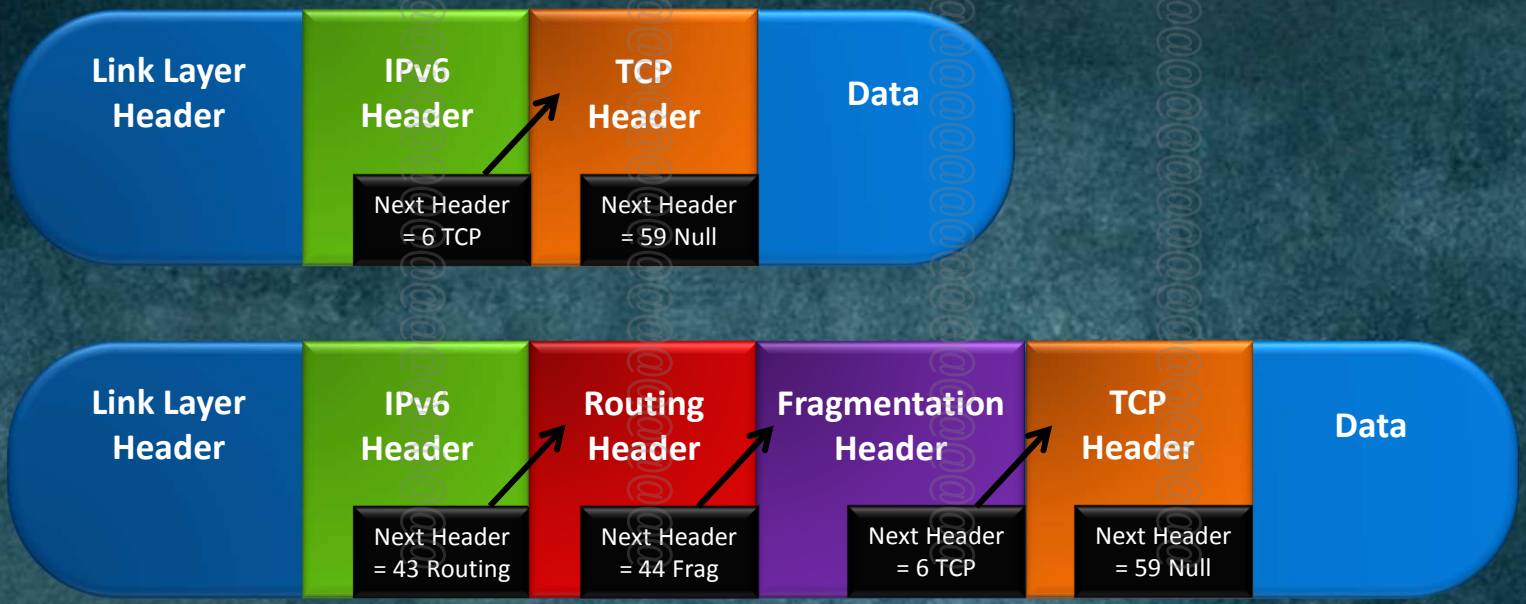


Extension Header

IPv6 utilizza l'Extension Header, campi opzionali di lunghezza fissa inseriti immediatamente dopo l'Header IPv6:

- Indicano il tipo di informazioni successive all'header stesso.

Gli Extension Header possono essere combinati anche se appaiono separati all'interno del singolo pacchetto, come nel seguente esempio:



Ordine in cui processare gli Extension Header

Vulnerabilità dell'Extension Header

La vantaggiosa flessibilità portata dagli Extension Header è ampiamente bilanciata da un corrispondente gamma di svantaggi, soprattutto in termini di sicurezza:

- Crearne una lista talmente grande da **sovraccaricare** il sistema che la gestisce;
- Ingrandire l'header fino alla **frammentazione del payload** evitando il controllo della seconda parte da eventuali firewall.

Il firewall non considera una minaccia la presenza di tali extension header, quindi non effettua nessun tipo di controllo su di essi:

- L'unico mezzo per **difendersi** è utilizzare prodotti altamente specializzati nell'applicazione di **regole specifiche** oppure **filtrare totalmente** l'extension header.

Gli Extension Header su cui bisognerebbe avere un'attenzione speciale sono:

- Routing header
- Fragmentation header

Routing Header

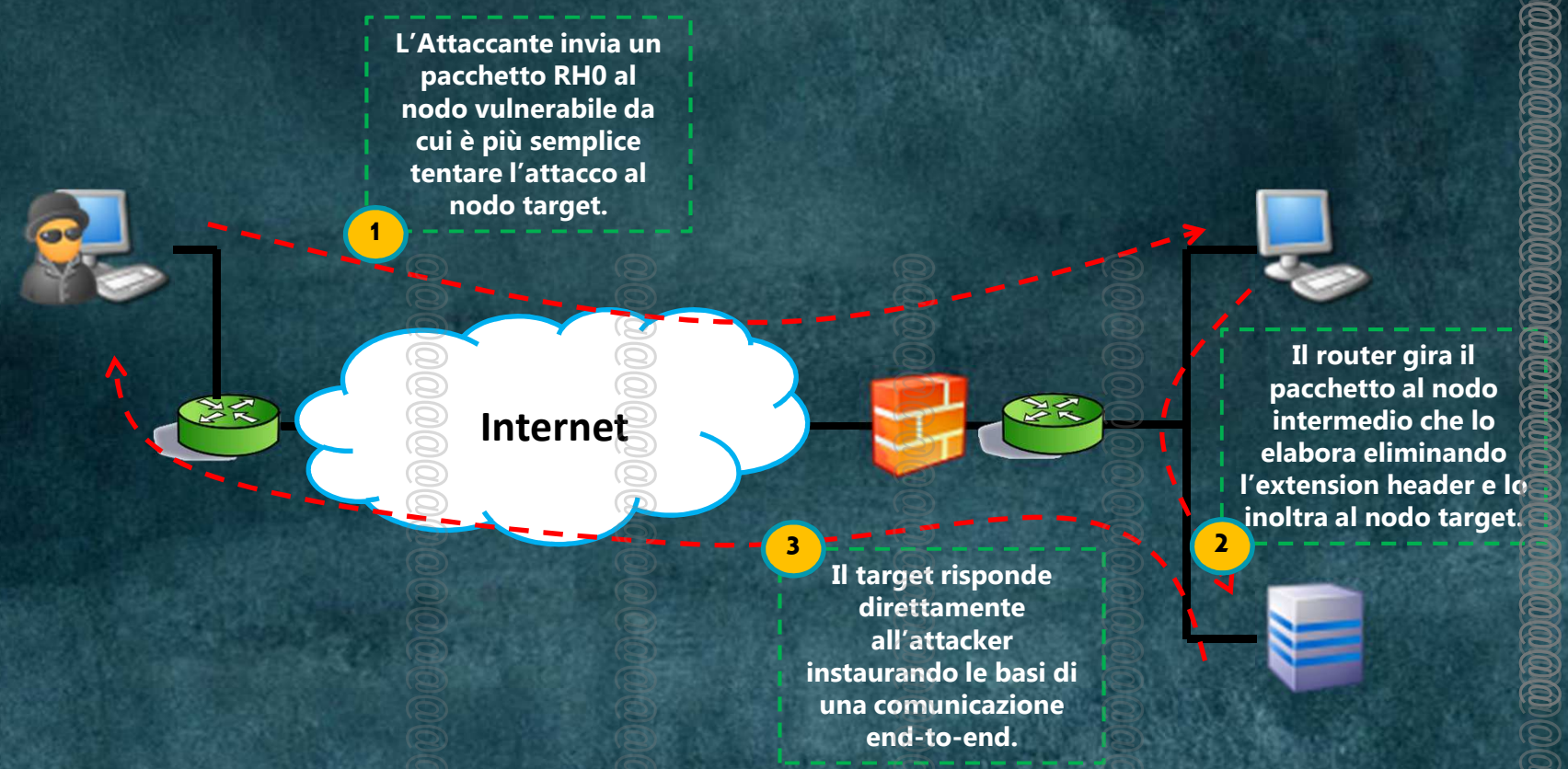
Permette di specificare in maniera più stringente, all'interno dell'header, il tragitto del pacchetto, invece di affidarlo al routing dinamico (**source routing**).

Il routing header si divide in due tipologie:

- **RH0**, che ha le stesse funzionalità dei source routing in IPv4;
- **RH2**, dedito al Mobile IPv6.

Oltre ad **aumentare** l'impiego di **risorse elaborative**, potrebbe essere usato per apportare pericolosi attacchi DoS e Bounded al sistema.

Routing Header



Routing Header

Il **bounded attack** consiste nell'inserimento di una o più destinazioni molteplici volte, in modo da far letteralmente rimbalzare il pacchetto tra i vari nodi, consumandone le risorse (effetto ping-pong).

Oggi come oggi, molti sistemi operativi hanno disabilitato RH0 di default e molti sistemi di sicurezza non permettono di default il passaggio degli RH0.

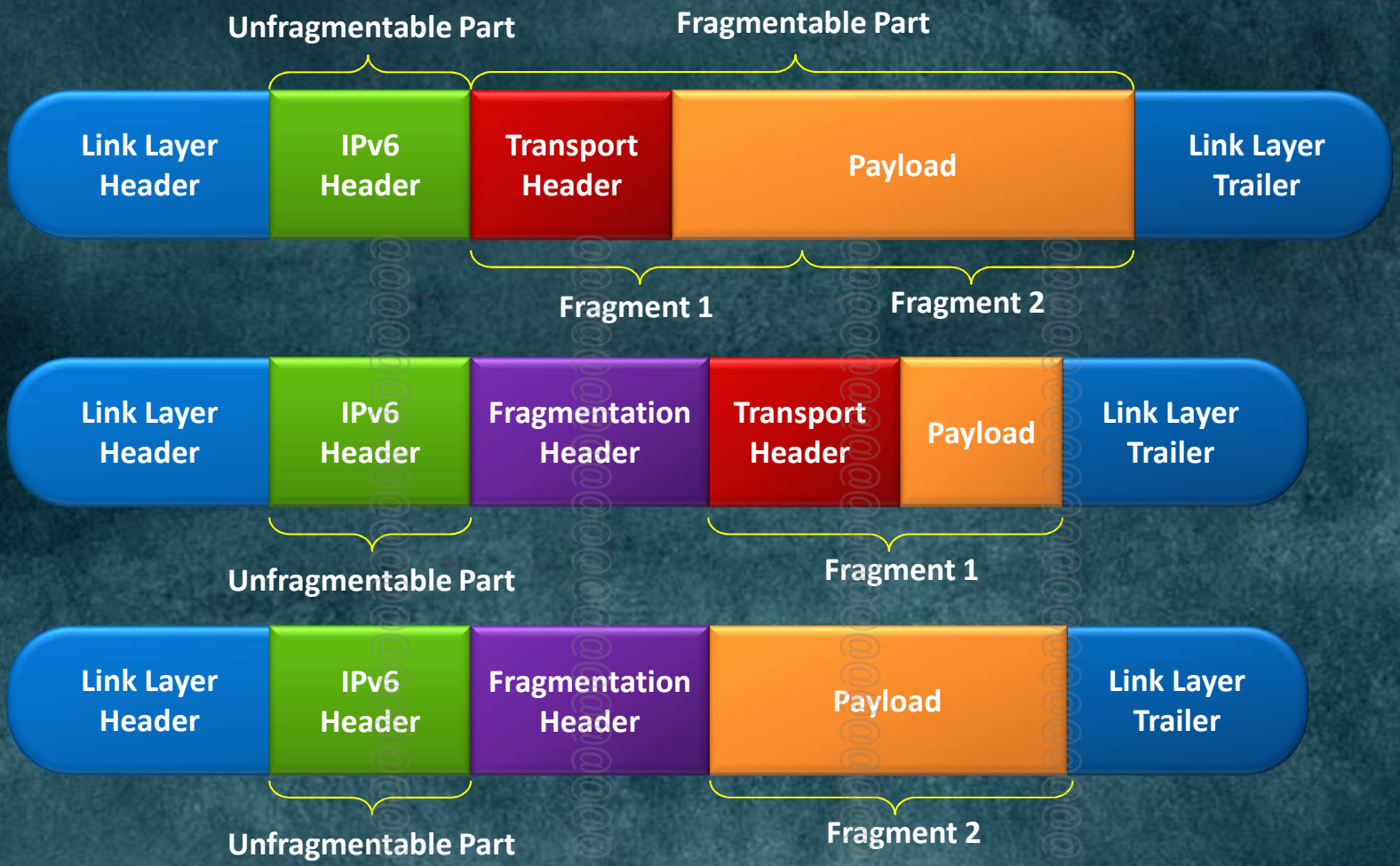
Fragmentation Header

La differenza sostanziale rispetto alla precedente versione consiste nell'impossibilità da parte dei router intermedi di effettuare la frammentazione:

- Sarà necessaria una fase iniziale di negoziazione (**Path MTU Discovery**) in cui stabilire correttamente l'MTU dei pacchetti (sfruttando le funzionalità dell'ICMPv6).

Nonostante ciò, anche il nuovo protocollo si trascina le medesime problematiche del suo predecessore, come ad esempio la possibilità di impostare un'MTU talmente bassa che nessun router possa dover effettuare un controllo attivo??

Fragmentation Header



Fragmentation Header: possibili Attacchi

- Si può sfruttare la frammentazione MTU per **inviare malware** alla macchina target, **nascondendoli** nei vari frame MTU, in questo modo l'host "d'appoggio" (successivo all'ostacolo), riassemblando i frammenti, accorgendosi che il contenuto raccolto è altro pacchetto non destinato a lui, va ad inoltrarlo verso il target vero e proprio;
- Si possono **attaccare le performance** del target, inviando degli MTU con frammenti mancanti che, lasciando in sospeso la comunicazione sul target, possano mandarlo in **overflow**(in realtà esistono tecniche più rapide ed efficienti per raggiungere questo obiettivo);
- È possibile effettuare una **discovery della topologia della rete** attraverso l'ausilio del ICMPv6, in particolare testando il percorso da MTU di grandezza eccessiva, a scalare. Ogni router intermedio che non dispone di un link di tali capacità invierà un **ICMPv6** " **Packet too Big** " al mittente malevolo, che può così ricostruirsi la topologia del percorso.

Fragmentation Header

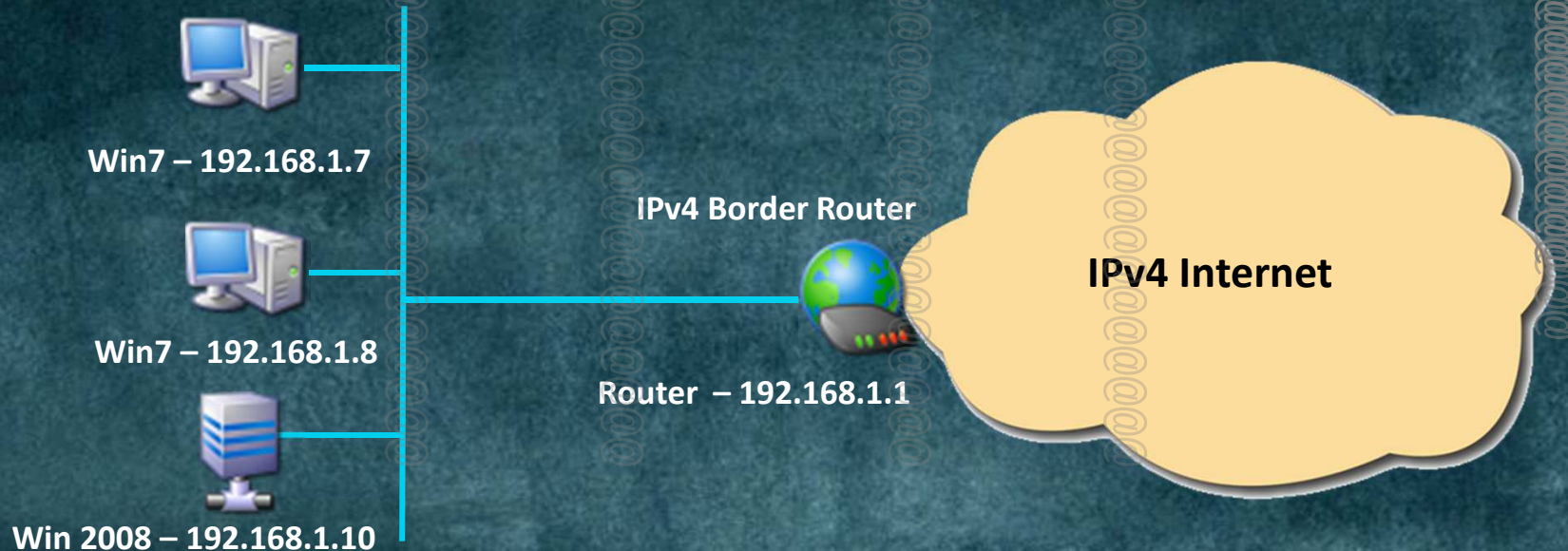
Solitamente l'MTU IPv6 è di 1280 bytes o superiore.

Qualsiasi MTU al di sotto dei 1280 bytes probabilmente è un tentativo di attacco, quindi sarebbe buona regola configurare i firewall con appropriate Access Control List (ACL) per non permettere il passaggio di MTU inferiori a 1280 Byte.

In realtà questa tecnica di mitigazione non è banale da applicare se si vuole preservare l'integrità e l'efficienza delle comunicazioni, in quanto sicuramente anche ogni MTU dell'ultimo frammento di un pacchetto sarà inferiore di 1280 byte, quindi sarà filtrata anch'essa e il pacchetto intero in questione rimarrebbe in standby.

SLAAC Attack

- Questa prova di concetto permette di attaccare le comunicazioni dual-stack di macchine Windows 7, ma l'attacco può essere condotto a danno anche di altri Sistemi Operativi che hanno il socket IPv6 installato e attivo di default.
- Vediamo lo schema logico

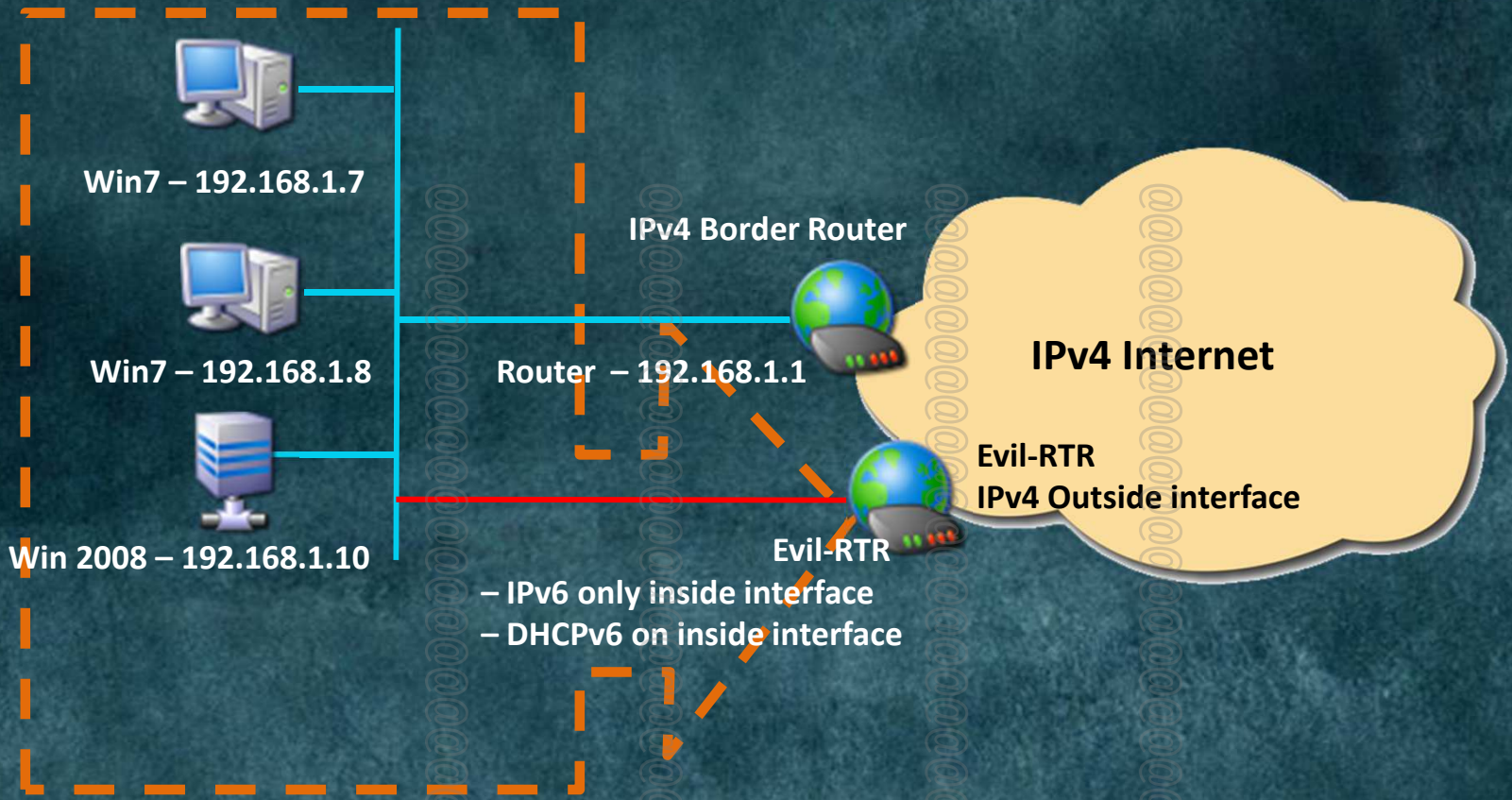


Schema dell'Attacco

- Fin qui nulla di nuovo ogni elemento lavora in IPv4 e il Border Router permette l'inoltro delle comunicazioni degli host privati attraverso il NAT.
- In questo senso ipotizziamo che il nostro router sia anche stato opportunamente hardenizzato evitando ARP Poisoning e MITM.
- Quello che andremo ora a fare è introdurre un Router "evil-rtr", nel network che abbiamo visto.
- Evil-RTR ha due interfacce di rete:
  - Un'interfaccia IPv6 only che si affaccia alle macchine vittima
  - una interfaccia IPv4 only che si affaccia a Internet.

- Il nostro obiettivo è usare Evil-RTR per creare un network IPv6 all'interno della rete che possa essere completamente sotto il nostro controllo come illustrato nello schema seguente.

Schema dell'Attacco SLAAC



Schema dell'attacco

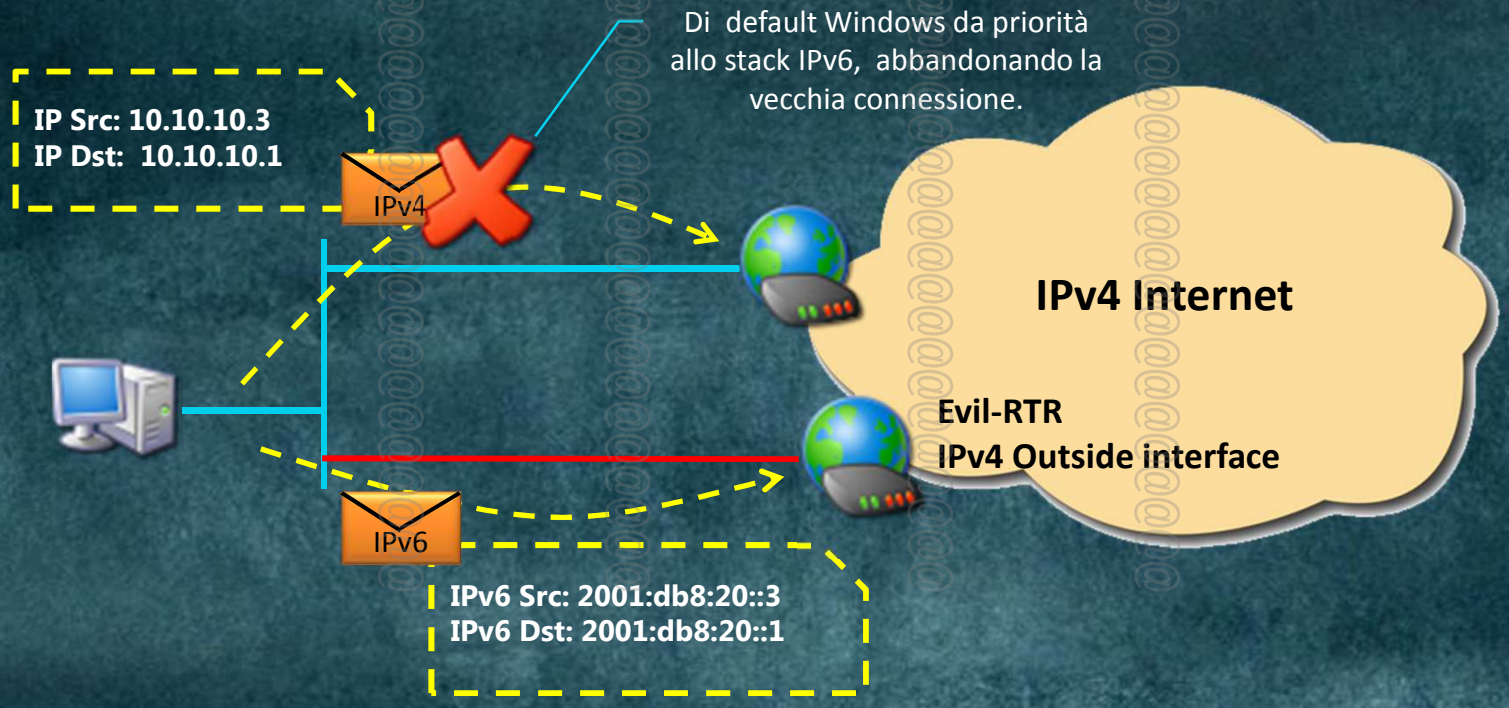
- Evil-RTR invierà degli RA al network locale causando agli host vittima un mutamento dell'indirizzamento IPv6 e della tabella di routing.
- Questo anche grazie all'attivazione del DHCPv6 sull'host attaccante.
- In aggiunta l'attaccante potrà attivare anche un DNS Malevolo, annunciato via DHCPv6.
- Quello che poi non è fatto è stato attivare un'interfaccia pubblica in IPv6 per Internet, cosa che avrebbe creato potenziali evidenze dell'attacco.
- Evil-RTR permetterà quindi agli host IPv6 di navigare nattati da IPv4.

Le conseguenze dell'Attacco

- **Grazie ai Routing Advertisement Evil-RTR attiverà e gestirà la connettività IPv6 delle vittime. In aggiunta esse "conosceranno" un DNS che verrà fornito da Evil-RTR.**
- **Per assicurare il completo controllo del network IPv6 in modo trasparente** all'utente **è importante che Evil-RTR abbia abilitato il** NAT-PT,
  NAT-PT è sistema ormai abbandonato dalla IETF, per far convivere IPv4 e IPv6, ma che può essere da noi riesumato, sicuri del risultato.
- In sostanza NAT-PT offre la possibilità di far convivere le due reti attraverso dei punti di NAT che assicurino la traduzione corretta IPv6 a IPv4 e viceversa.
- Grazie a questo meccanismo possiamo realizzare in modo semplice ed efficace l'attacco
- *Per eventuali approfondimenti trovate qui un paper opportuno.*

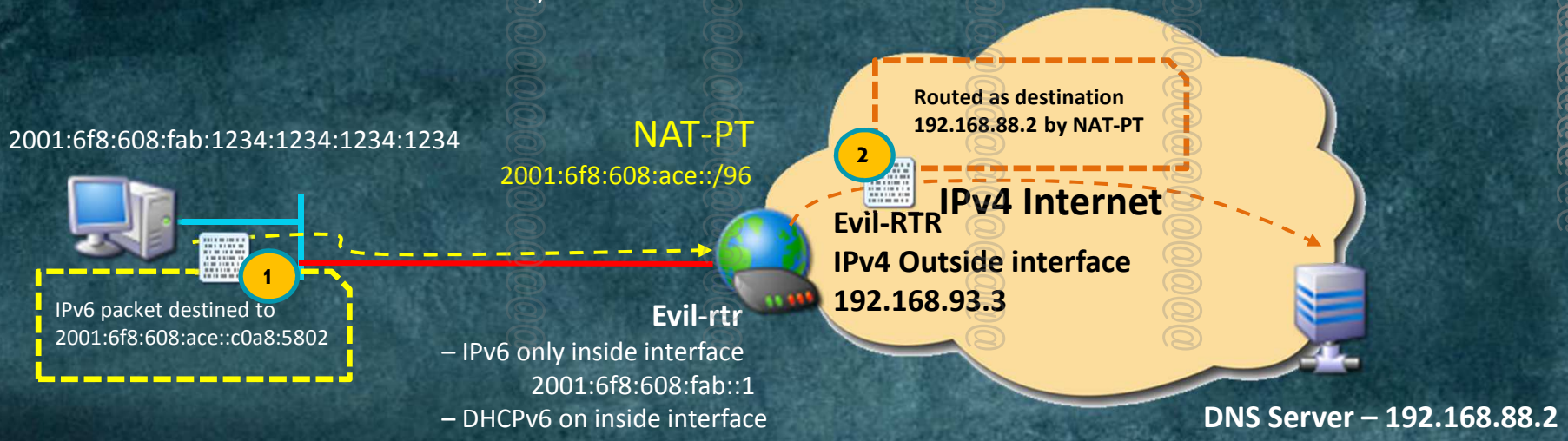
Le conseguenze dell'Attacco

- Per usare NAT-PT occorre definire un prefisso off-link /96.
- Un qualsiasi segmento di IP può essere scelto, purché routabile pubblicamente.
- Ogni indirizzo di destinazione intercettato dal NAT-PT che risponda a questo prefisso sarà interpretato come un indirizzo IPv6 con un indirizzo IPv4 embedded nei suoi ultimi 32 bit.



Esempio di NAT-PT

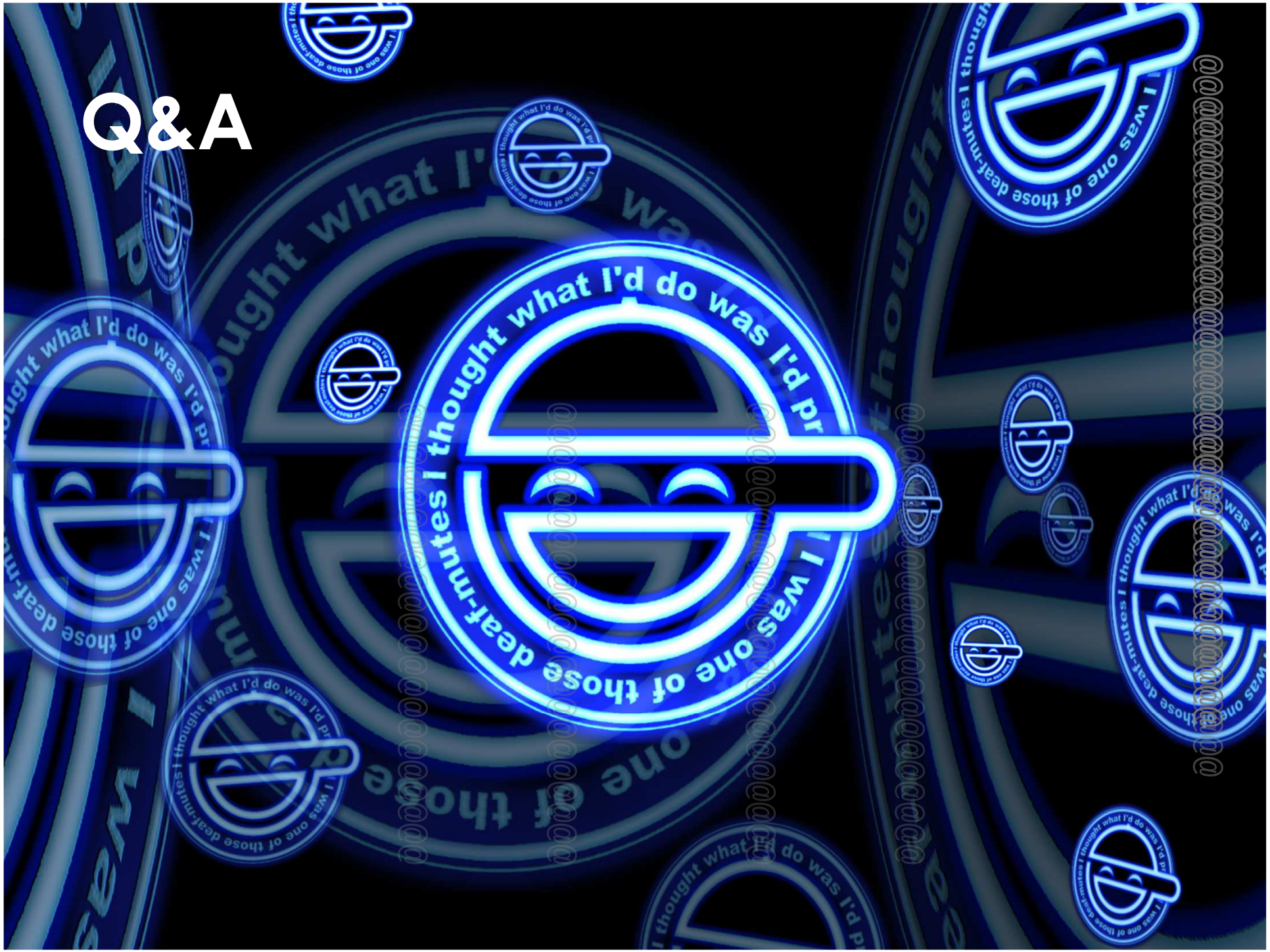
- Esempio.
  - Io posso configurare il mio NAT-PT box con un prefisso quale 2001:6f8:608:ace::/96.
  - L'indirizzo IPv6 del DNS server che indicherò via DHCPv6 è: 2001:6f8:608:ace::c0a8:5802.
  - Questo indirizzo cade all'interno del prefisso definito quindi se il NAT-PT vede un traffico destinato ad esso gli ultimi 32 bits (c0a8:5802) saranno estratti e traslati nel vero indirizzo IPv4 del Server, ovvero 192.168.88.2.



Attivazione dell'attacco…

- Ci siamo quasi...
- Con il NAT-PT attivato, Evil-RTR può ora offrire una path logica per la rete Internet IPv4 alle vittime connesse via IPv6.
- Se questo causa lo swap del flusso principale di comunicazione ad Internet della vittima via IPv6 attraverso Evil-RTR (al posto del precedente traffico IPv4 attraverso il legittimo Border Router) il nostro attacco SLAAC è riuscito.
- Grazie a Evil-RTR le nostre vittime hanno ora un duplice indirizzamento: IPv4 e IPv6 attivo e sono delle vere e proprie stazioni "dual stacked".
- Di default gli host "dual stack" preferiscono le reti IPv6 quando sono disponibili e questo assicura la riuscita dell'attacco nella stragrande maggioranza dei casi…

A questo punto vediamo lo SLAAC in azione…


Q&A

Thank you for your time

Licenza dell'opera

Gli autori:

- Stefano Maccaglia
- Matteo Dominizi

Eccetto dove diversamente indicato
quest'opera è rilasciata con licenza

http://creativecommons.org/licenses/by-nc-nd/2.5/it/