

| Decimal | Keyword | Version | Reference |
|---------|---------|-----------------------------|-----------------------|
| 0-1 | | Reserved | [Jon Postel][RFC4928] |
| 2-3 | | Unassigned | [Jon Postel] |
| 4 | IP | Internet Protocol | [RFC791][Jon Postel] |
| 5 | ST | ST Datagram Mode | [RFC1190][Jim Forgie] |
| 6 | IPv6 | Internet Protocol version 6 | [RFC1752] |
| 7 | TP/IX | TP/IX: The Next Internet | [RFC1475] |
| 8 | PIP | The P Internet Protocol | [RFC1621] |
| 9 | TUBA | TUBA | [RFC1347] |
| 10-14 | | Unassigned | [Jon Postel] |
| 15 | | Reserved | [Jon Postel] |

Franco Tinarelli
INAF – IRA

3 February 2011
IANA
exhausted its
IPv4 free pool

IPng
Internet Protocol
Next Generation

Pula – Cagliari
16 – 19/09/2014

IANA Internet Assigned Numbers Authority

Streaming Datagram Mode

IPv6

Internet Protocol version 6 (RFC2460)

- IPv6 node:** un dispositivo che implementa IPv6
- IPv6 Router:** un dispositivo in grado di instradare un pacchetto non indirizzato a se stesso
- IPv6 host:** ogni nodo che non è un router

- Maggiore capacità d'indirizzamento:
340.282.366.920.938.463.463.374.607.431.768.211.456
o per meglio dire 2^{128} o $3,4 \times 10^{38}$
- Semplificazione del formato dell'header:
lunghezza fissa di **40 Bytes** allineati a 8-ottetti
- Maggiore supporto per estensioni e opzioni
- Nuova capacità di "Flow Labeling"
- Nuova capacità di autenticazione e privacy
- Autoconfigurazione degli indirizzi
- Assenza del NAT

- ~~1883~~ → 2460 (tools.ietf.org/html/rfc2460)

Dec 1995

Dec 1998

è uno Standards Track ed è stato aggiornato da:

rfc 5095 (Dec 2007) Viene deprecato RHO (Routing Headers Type 0)

rfc 5722 (Dec 2009) Gestione degli Overlapping Fragments

rfc 5871 (May 2010) IANA: Linee guida per l'assegnazione dei Routing Headers

rfc 6437 (Nov 2011) Specificazione della Flow Label

rfc 6564 (Apr 2012) Un formato uniforme per gli Extension Headers

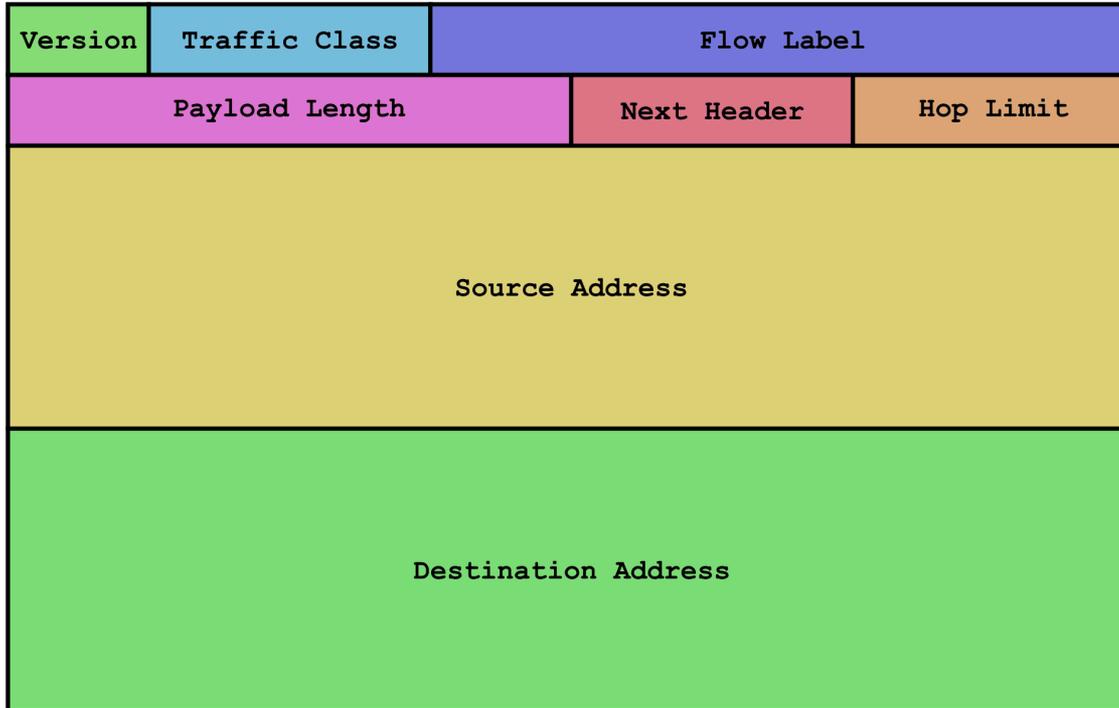
rfc 6935 (Apr 2013) IPv6 e UDP Checksums per i Tunneled Packets

rfc 6946 (May 2013) Elaborazione degli "Atomic" Fragments

rfc 7045 (Dec 2013) Trasmissione ed elaborazione degli Extension Headers

rfc 7112 (Gen 2014) Implicazioni del sovradimensionamento dell' Header Chains

Formato dell'Header IPv6



Lunghezza fissa di 40 Bytes

| | |
|---------------------|---------|
| Version | 4-bit |
| Traffic Class | 8-bit |
| Flow Label | 20-bit |
| Payload Length | 16-bit |
| Next Header | 8-bit |
| Hop Limit | 8-bit |
| Source Address | 128-bit |
| Destination Address | 128-bit |

Allineamento a 8 ottetti

- **Version** 4-bit numero di versione del Protocollo Internet = **6**
- **Traffic Class** 8-bit Classe del traffico (**default tutti i bit a 0**) impostata da chi genera il traffico e/o modificata dai routers che lo instradano. Identifica le diverse classi di priorità del pacchetto. I **Nodi che supportano** l'uso di una o più classi **possono modificare** questo campo, **i nodi che non sono in grado** di utilizzare la classe devono **lasciarla inalterata**.
- **Flow Label** 20-bit definisce la label della sequenza di pacchetti che richiedono ai routers attraversati un trattamento speciale, come il "real time" o una QOS diversa dal default. I dispositivi che non supportano tale opzione devono **impostarla a 0** generando il pacchetto, **non modificarla** se attraversati, **ignorarla** quando ricevono il pacchetto.

- **Payload Length** 20-bit unsigned integer. Lunghezza dei dati che seguono L'header in ottetti. Le eventuali estensioni dell'header sono comprese in questa lunghezza.
- **Next Header** 8-bit specifica il tipo dell'extension header che segue L'header IPv6. I valori sono identici a quelli IPv4 e sono registrati da IANA (<http://www.iana.org/assignments/ip-parameters/>) e non più dal rfc1700. **No Next Header ha valore 59.**
- **Hop Limit** 8-bit unsigned integer. Decrementato di 1 da ogni nodo Attraversato. Scartato se decrementato a 0.
- **Source Address** 128-bit indirizzo del generatore del pacchetto.
- **Destination Address** 128-bit indirizzo del nodo di destinazione (**può non essere l'ultima destinazione** se è presente un routing header)

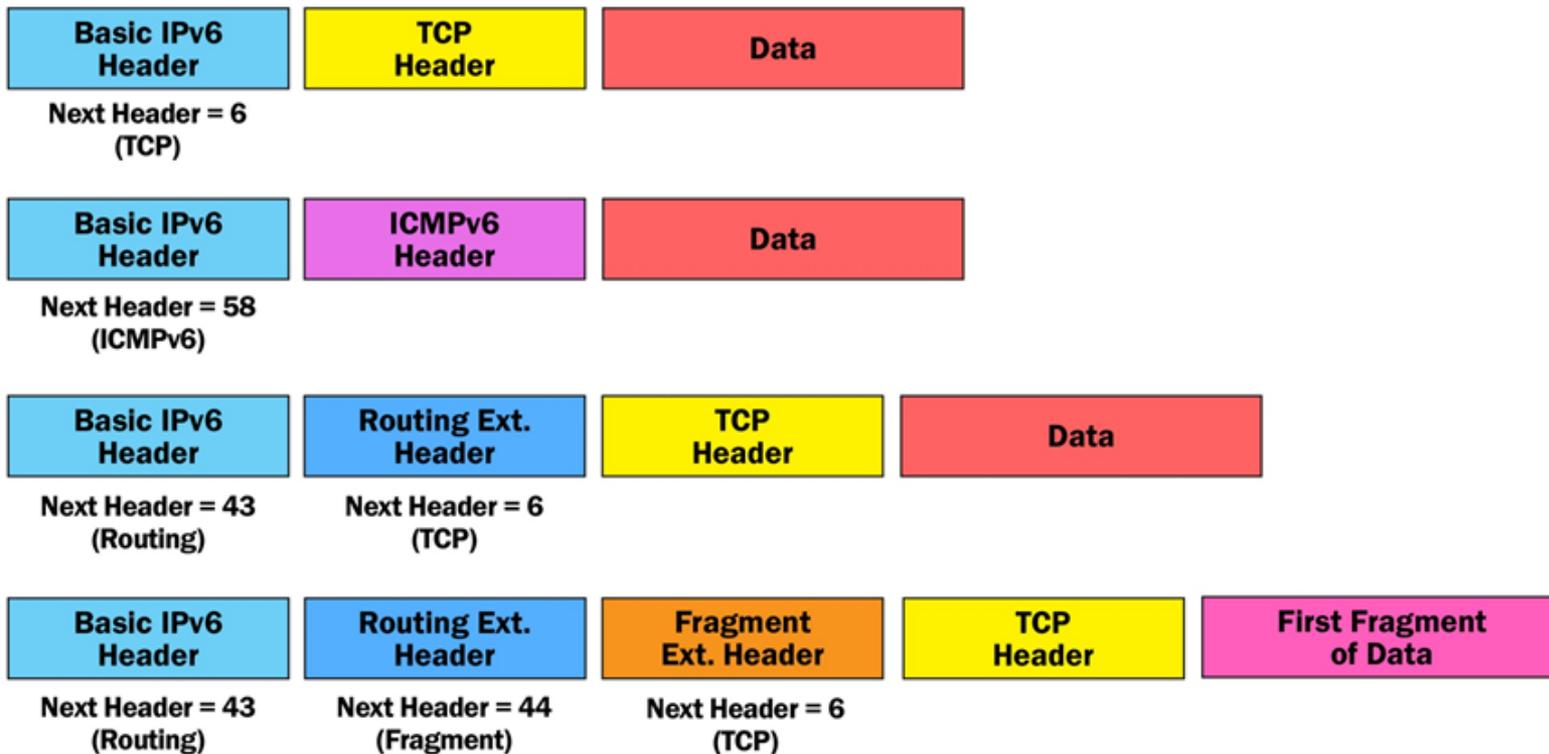
Formato dell'Header IPv4

Lunghezza variabile e allineamento a 32 bit

| | | | | |
|---------------------|----------|-----------------|-----------------|--|
| Version | IHL | ToS | Total Length | |
| Identification | | Flgs | Fragment Offset | |
| Time To Live | Protocol | Header Checksum | | |
| Source Address | | | | |
| Destination Address | | | | |
| Options | | | Padding | |

I campi in bianco non esistono più nell'header IPv6.

Le opzioni sono State sostituite Dagli Extensions Headers.



| Protocol Number | Description | Reference |
|-----------------|-------------------------------------|--------------------|
| 0 | IPv6 Hop-by-Hop Option | [RFC2460] |
| 43 | Routing Header for IPv6 | [RFC2460][RFC5095] |
| 44 | Fragment Header for IPv 6 | [RFC2460] |
| 50 | Encapsulating Security Payload | [RFC4303] |
| 51 | Authentication Header | [RFC4302] |
| 60 | Destination Options for IPv6 | [RFC2460] |
| 135 | Mobility Header | [RFC6275] |
| 139 | Host Identity Protocol | [RFC5201] |
| 140 | Shim6 Protocol | [RFC5533] |
| 253 | Use for experimentation and testing | [RFC3692][RFC4727] |
| 254 | Use for experimentation and testing | [RFC3692][RFC4727] |

- Gli **Extensions Header** devono essere processati in **modo sequenziale** dal primo all'ultimo;
- **Solo** l'Host **destinatario** del pacchetto può processare gli Extensions Header;
- Unica eccezione l'**Hop-by-Hop** Options Header che viene trattato da **tutti i nodi** attraversati, sorgente e destinazione compresi. Se presente è il primo dopo l'IPv6 Header che lo segnala col **valore 0** nel **Next Header Field**;
- Se processando un Next Header il nodo non lo riconosce, deve **scartare tutto il pacchetto** e segnalare l'errore al nodo sorgente con un pacchetto ICMP. Stesso comportamento se si incontra un valore 0 di Next Header in un Header diverso dal principale.
- Ogni **Extensions Header** e' un intero **multiplo di 8 ottetti** per permettere l'allineamento naturale dei successivi. Ogni campo dell'header viene allineato ad un multiplo della sua lunghezza in ottetti (1 – 2 – 4 – 8).

- La completa implementazione del protocollo IPv6 richiede la presenza dei seguenti **Extensions Header** (vedi anche rfc 5095, rfc5871, rfc6564, rfc7045, rfc7112)
 - **Hop-by-Hop Options**
 - **Routing [deprecato il Type 0 con rfc 5095** (la possibilità di indicare più volte lo stesso indirizzo crea un'oscillazione del pacchetto tra due nodi generando una congestione su tutta la tratta.) nel 2009 **deprecato il Type 1]**
 - **Fragment**
 - **Destination Options**
 - **Authentication (rfc ~~1826-2402~~ 4302)**
 - **Encapsulating Security Payload (rfc ~~1827-2406~~ 4303)**

- Quando in un pacchetto vengono usati più Extensions Header, si raccomanda che compaiano una sola volta (tranne il Destination Options header) nel seguente ordine:
 - **IPv6 header**
 - **Hop-by-Hop Options header**
 - **Destination Options header** (per la prima destinazione più le successive contenute nel Routing header)
 - **Routing header**
 - **Fragment header**
 - **Authentication header**
 - **Encapsulating Security Payload header**
 - **Destination Options header** (solo per la destinazione finale)
 - **Upper-layer header (tcp, udp, icmp, etc.)**

- Due degli extension header appena citati, il **Hop-by-Hop** Options header e il **Destination** Options header, contengono un numero variabile di opzioni di tipo **TLV (type-length-value)** nel formato:



- **Option Type** 8-bit che descrivono il tipo di opzione
- **Opt Data Len** 8-bit unsigned integer, specifica la lunghezza dei dati in ottetti
- **Option Data** Lunghezza variabile, contiene i dati dell'opzione

Le opzioni all'interno dell'header **devono** essere **processate sequenzialmente**.

L'**Option Type** è codificato in modo che i primi **due bit più significativi** specifichino l'**operazione** da compiere **se il nodo** di destinazione **non riconosce** l'opzione:

00 - ignora e **continua** | **01** – **scarta** il pacchetto | **10 scarta** il pacchetto e **invia ICMP** Codice 2

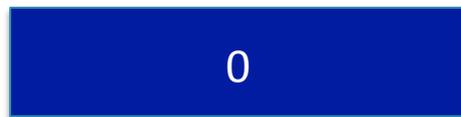
11 – **scarta** il pacchetto e **invia ICMP** Codice 2 solo se la destinazione **non è** un indirizzo **multicast**

Il **terzo bit** più significativo specifica la possibilità di **modifica** delle **Options Data** durante la fase di routing: **0** – **non** può cambiare | **1** – **può** cambiare.

I tre bit più significativi sono comunque parte integrante degli 8 bit del tipo di opzione, la stessa numerazione vale sia per Hop-by-Hop header sia per Options header, anche se opzioni particolari sono utilizzabili solo in uno dei due headers.

In questo rfc vengono definite due opzioni di padding necessarie per l'allineamento agli 8 ottetti: **Pad1 (00000000)** e **PadN (00000001)**

Pad1 – opzione di formato speciale senza campi di lunghezza e valore.



Viene usata per inserire un solo ottetto di padding nella Options area di un header. Se è richiesto **più di un ottetto** per allineare l'opzione bisogna utilizzare **PadN** invece di più opzioni Pad1.

PadN – l’opzione è utilizzata per inserire due o più ottetti d’allineamento. Per **N** ottetti di padding il campo **Opt Data Len** contiene **N-2** e il campo **Option Data** è formato da **N-2** ottetti di valore **0**.



Una Options con i campi allineati ad un multiplo della loro lunghezza in ottetti (1 – 2 – 4 – 8) viene rappresentata come nell’esempio che segue:

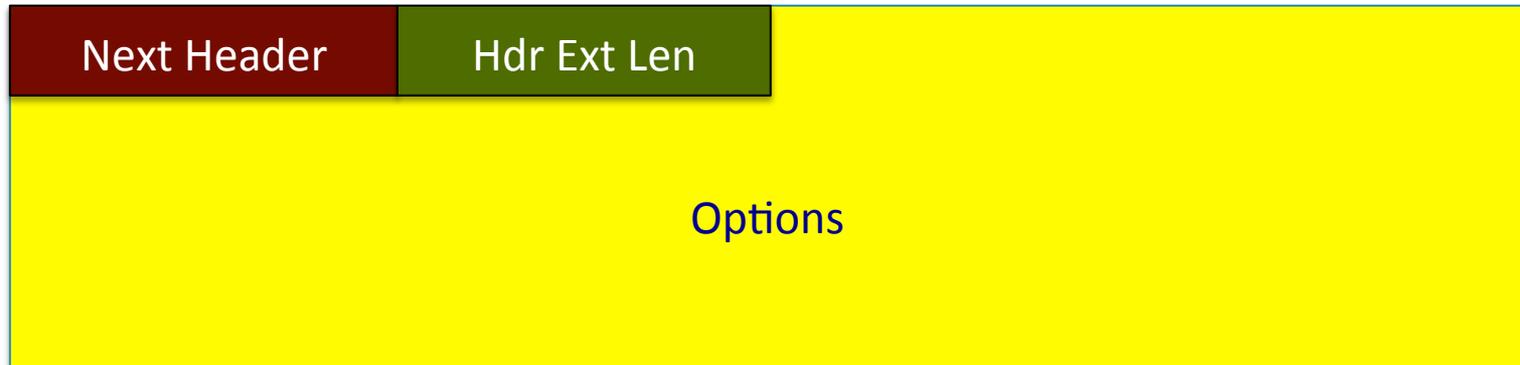


L'**Hop-by-Hop** e il **Destination Options** header hanno la stessa struttura, il primo identificato da uno **0** nel Next Header dell'IPv6 header, il secondo dal valore **60**.

Next Header 8-bit. Valore del tipo di header che segue il presente.

Hdr Ext Len 8-bit unsigned. Lunghezza dell'Options Header in unità di 8-ottetti, senza includere il primo.

Options Lunghezza variabile. La lunghezza totale dell'header deve essere multipla di 8 ottetti. Contiene una o più opzioni codificate TLV.

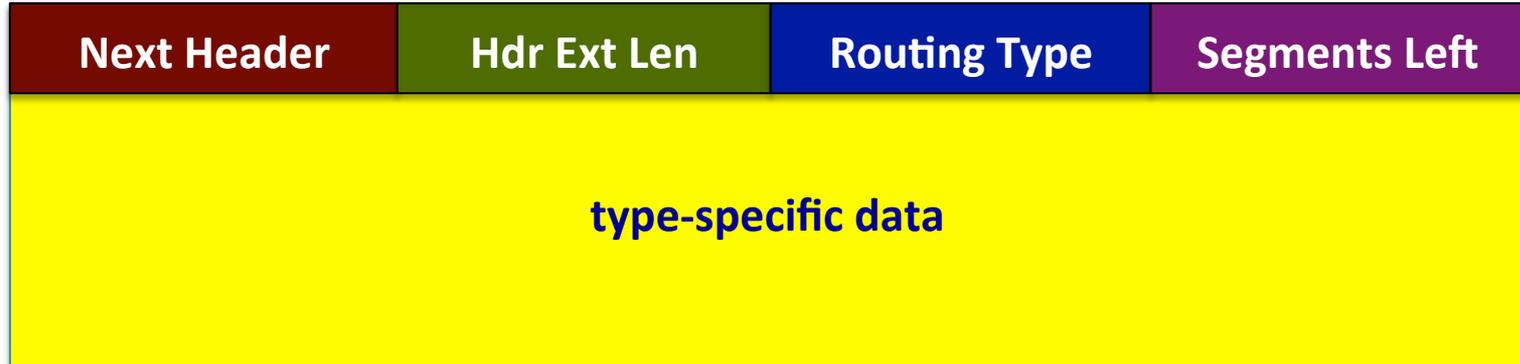


IPv6 IPv6 Specifications (rfc2460) Extension Headers + Options

Esempio di Options Header contenente due opzioni TLV

| | | | |
|----------------|----------------|-----------------|---------------|
| Next Header | Hdr Ext Len=3 | 0 | Option Type=Y |
| Opt Data Len=7 | 1 ottetto | 2 ottetti | |
| 4 ottetti | | | |
| PadN Option=1 | Opt Data Len=4 | 0 | 0 |
| 0 | 0 | Opt Data Len=12 | Option Type=X |
| 4 ottetti | | | |
| 8 ottetti | | | |

Il **Routing header** (tipo **43**) è usato da una sorgente IPv6 per indicare uno o più nodi intermedi da attraversare prima di raggiungere il nodo di destinazione.



- Routing Type** 8-bit. Tipo di routing header (**deprecati 0 e 1**, attivi 2 e 3).
- Segment Left** 8-bit unsigned. Numero dei segmenti di route rimanenti. Nodi intermedi ancora da visitare prima di raggiungere la destinazione.
- type-spec data** Lunghezza variabile. Formato definito dal tipo di routing, la lunghezza totale dell'header deve essere multipla di 8 ottetti.

IPv6 IPv6 Specifications (rfc2460) Extension Headers Fragment header

- Il Fragment Header (tipo **44**) è utilizzato da una sorgente IPv6 per inviare un pacchetto che non può essere contenuto nelle MTU dei nodi da attraversare, per giungere a destinazione.
- **Il pacchetto può essere frammentato solo dal nodo sorgente, contrariamente a quello che accade in IPv4.**
- Per ogni pacchetto che deve essere frammentato, il nodo sorgente genera un'identificativo che deve essere diverso da quello di un pacchetto frammentato di recente con stesso indirizzo di sorgente e destinazione. Se è presente un Routing header, il nodo destinazione coincide con la destinazione finale.
- Per “frammentato di recente” si intende un tempo che si avvicina al massimo di vita del pacchetto, compreso il tempo di transito dalla sorgente alla destinazione e quello speso per riassemblare i frammenti dello stesso pacchetto. Non essendo richiesto di conoscere questo tempo, l'Identificativo può essere un semplice contatore “wrap-around” di 32 bit incrementato tutte le volte che un pacchetto debba essere frammentato.
- **In IPv6 la minima MTU utilizzabile è di 1280 ottetti.**

IPv6 IPv6 Specifications (rfc2460) Extension Headers Fragment header

- Il **Fragment header** è identificato da un valore di Next Header uguale a **44** e ha il seguente formato:



- Next Header** 8-bit. Identifica il tipo dell'header iniziale della parte frammentabile del pacchetto originale.
- Reserved** 8-bit. Inizializzati a 0 per la trasmissione, ignorati alla ricezione.
- Fragment Offset** 13-bit unsigned int. Offset in unità di 8-ottetti dei dati che seguono l'header, relativo all'inizio della parte frammentabile del pacchetto originale.
- Res** 2-bit. Inizializzati a 0 per la trasmissione, ignorati alla ricezione.
- M** Flag. **1** = ancora frammenti; **0** = ultimo frammento

IPv6 IPv6 Specifications (rfc2460) Extension Headers Fragment header

- Il **pacchetto iniziale**, troppo grande e non ancora frammentato, consiste di **due parti**:
 - La **parte non frammentabile** che contiene l'header IPv6 più ogni extension headers che deve essere processato dai nodi attraversati fino alla destinazione.
 - La **parte frammentabile** è il resto del pacchetto cioè ogni extension headers che deve essere processato solo dalla destinazione, l'upper-layer header e i dati.
- La **parte frammentabile** del pacchetto originale deve essere divisa in frammenti multipli di 8-ottetti ad eccezione dell'ultimo frammento.

IPv6 IPv6 Specifications (rfc2460) Extension Headers Fragment header

- i **frammenti** sono trasmessi in separati “**fragment packets**” come illustrato:
 - **Pacchetto originale:**



- **Pacchetti frammentati:**



IPv6 IPv6 Specifications (rfc2460) Extension Headers **Fragment header**

- La parte non frammentabile avrà la **Payload Length cambiata** rispetto all'header IPv6 originale e conterrà la lunghezza del pacchetto frammentato, meno la lunghezza dell'header IPv6. Il valore dell'ultimo campo di **Next Header** verrà modificato in **44**.
- Il **Fragment header** avrà' come **valore** del campo di:
 - **Next Header** quello del **primo header** della parte **frammentabile** del pacchetto originale.
 - **Fragment Offset** conterrà il valore relativo all'inizio della parte frammentabile del pacchetto originale, **nel primo frammento varrà 0**
 - IL flag **M** avrà valore **0** nell'**ultimo** frammento e **1** in tutti **gli altri**
 - **Identification** assumerà il valore generato per il pacchetto originale.
- Il **pacchetto ricostruito** imposterà il Next Header dell'ultimo header della parte non frammentabile al valore di quello contenuto nel Fragment header del primo pacchetto frammentato, il Payload Length verrà ricalcolato e la posizione dei singoli frammenti ricavata dai loro offset.

IPv6 IPv6 Specifications (rfc2460) Extension Headers Fragment header

- Se Entro **60 secondi** dall'arrivo del primo pacchetto non sono arrivati tutti i frammenti, l'operazione di ricostruzione viene interrotta e i frammenti scartati. Se è arrivato il primo pacchetto (offset 0) un ICMP Time Exceeded verrà inviato al nodo generatore del frammento.
- Se la **lunghezza di un frammento**, ricavata dal campo Payload Length e con il Flag **M** a **1**, non è multipla di 8-ottetti, il frammento viene scartato e un ICMP Parameter Problem (valore 0) che punta al Payload Length viene inviato al nodo generatore del frammento.
- Se la **lunghezza e l'offset** di un frammento è tale che la lunghezza del pacchetto ricostruito **supera i 65535 ottetti**, il frammento è scartato e un ICMP Parameter Problem (valore 0) che punta al Fragment Offset viene inviato al nodo generatore del frammento.

- ~~1884~~ → ~~2373~~ → ~~3513~~ → 4291 (tools.ietf.org/html/rfc4291)
Dec 1995 Jul 1998 Apr 2003 Feb 2006

rfc 4291 è uno Standards Track ed è stato aggiornato da:

rfc 5952 (Aug 2010) Recommendation for IPv6 Address Text Representation

rfc 6052 (Oct 2010) IPv6 Addressing for IPv4/IPv6 Translators

rfc 7136 (Feb 2014) Significance of IPv6 Interface Identifier

- Queste specifiche definiscono l'architettura dell'indirizzo IPv6 e contengono il formato base per i diversi tipi di indirizzo:
- **UNICAST**: un identificativo per una singola interfaccia. Un pacchetto inviato ad un indirizzo unicast è consegnato **all'interfaccia** contrassegnata da questo indirizzo.
- **ANYCAST**: Un identificativo per un gruppo d'interfacce (tipicamente appartenenti a nodi diversi). Un pacchetto inviato ad un indirizzo anycast è consegnato **ad una delle interfacce** contrassegnate da questo indirizzo, la più vicina secondo la misura di distanza del protocollo di routing.
- **MULTICAST**: Un identificativo per un gruppo d'interfacce (tipicamente appartenenti a nodi diversi). Un pacchetto inviato ad un indirizzo multicast è consegnato **a tutte le interfacce** contrassegnate da questo indirizzo. Sostituisce l'indirizzo di broadcast che non esiste in IPv6.

- La rappresentazione di un indirizzo IPv6 si avvale di **8 campi** di due ottetti in **notazione esadecimale** separati dal carattere :
 - **aaa:bbb:ccc:ddd:eee:fff:0000:1111**
- In IPv6 ogni campo dell'indirizzo può contenere tutti 0 (0x0000) o tutti 1 (0xffff).
- Gli indirizzi IPv6 di ogni tipo sono assegnati alle interfacce e non ai nodi, qualsiasi indirizzo unicast assegnato alle interfacce di un nodo può essere usato come identificativo di quel nodo.
- Tutte le interfacce devono avere almeno un indirizzo unicast di Link-Local
- Una singola interfaccia può avere più indirizzi IPv6 di ogni tipo (unicast, anycast e multicast) e di ogni scopo.

Nel rfc 4291 esiste una grande flessibilità nella composizione testuale dell'indirizzo IPv6, nell'esempio sono indicate diverse rappresentazioni dello stesso indirizzo:

2001:0db8:0000:0000:0001:0000:0000:0001

2001:db8:0:0:1:0:0:1

2001:0db8:0:0:1:0:0:1

2001:db8::1:0:0:1

2001:db8::0:1:0:0:1

2001:0db8::1:0:0:1

2001:db8:0:0:1::1

2001:db8:0000:0:1::1

2001:DB8:0:0:1::1

Nelle diverse sintassi si nota la presenza di regole di semplificazione, se ne riportano le raccomandazioni contenute nel rfc 5952 che ha aggiornato il 4291:

- Un gruppo di 16 bit a zero 0000 **deve** essere rappresentato da un unico **0**
da 2001:0db8:0000:0000:0001:0000:0000:0001
a **2001:0db8:0:0:0001:0:0:0001**
- In un gruppo di 16 bit gli zero che precedono **devono** essere **eliminati**
da 2001:0db8:0:0:0001:0:0:0001
a **2001:db8:0:0:1:0:0:1**

- Gruppi di 16 bit a zero e adiacenti devono essere sostituiti da “::” seguendo la regola della massima semplificazione. Se in un indirizzo esistono più gruppi a zero la sostituzione interviene su quello **più numeroso**, in caso di pari lunghezza interviene sul gruppo **più a sinistra**. Non è possibile sostituire un unico gruppo di 16 bit a 0:
da 2001:db8:0:0:1:0:0:1
a **2001:db8::1:0:0:1**
- Nella composizione dell'indirizzo Sono ammesse **solo** le lettere (a,b,c,d,e,f) **minuscole**

- Indicazioni per la sintassi indirizzo più numero di porta:

[2001:db8::1]:80 RACCOMANDATO (default)

~~2001:db8::1:80~~ NON RACCOMANDATO perchè ambiguo

2001:db8::1.80

2001:db8::1 port 80

2001:db8::1p80

2001:db8::1#80

- La rappresentazione testuale del prefisso di un indirizzo IPv6 segue le regole del Classless Inter-Domain Routing (CIDR)[rfc4632]:

prefisso-IPv6/lunghezza-prefisso

- **prefisso-IPv6:** indirizzo testuale nelle notazioni precedentemente definite.
- **Lunghezza-prefisso:** è un valore decimale che indica la lunghezza della parte di prefisso dell'indirizzo.

2001:db8:0:cd30::/60

- La rappresentazione di un indirizzo IPv6 e del suo prefisso può essere semplificata in

2001:db8:0:cd30:123::cdef/60

| Tipo d'indirizzo | Notazione binaria | Notazione IPv6 |
|--------------------|----------------------|----------------|
| Unspecified | 00...0 (128 bits) | ::/128 |
| Loopback | 00...1 (128 bits) | ::1/128 |
| Multicast | 11111111 (8 bits) | FF00::/8 |
| Link-Local Unicast | 1111111010 (10 bits) | FE80::/10 |
| Global Unicast | Tutto il resto | IANA Registry |

Per ora l'unico prefisso assegnato da IANA al Global Unicast è

2000::/3 [3fff::/3]

00100000 00000000 [00111111 11111111]

- **Unspecified Address: 0:0:0:0:0:0:0:0 ::/128**
Non può essere assegnato a nessun nodo.
Indica l'assenza di un indirizzo, viene usato nel pacchetto sorgente di un nodo che deve ancora acquisire l'indirizzo.
Non può essere usato come indirizzo destinazione in un pacchetto IPv6 o in un Routing headers IPv6.
Non può essere rilanciato da un router IPv6. Viene usato nella configurazione statica di un Router IPv6 per definire la destinazione di default.
- **Loopback Address: 0:0:0:0:0:0:0:1 ::1/128**
È utilizzato da un nodo per inviare un pacchetto IPv6 a se stesso e non può essere utilizzato come indirizzo d'una interfaccia fisica ma solo della "loopback interface" tipicamente **lo0**
Non può essere utilizzato in un pacchetto destinato all'esterno del singolo nodo o rilanciato da un Router IPv6.
Un pacchetto con destinazione un indirizzo di loopback e ricevuto da una interfaccia fisica deve essere scartato.

| IPv6 Prefix | Allocation | Reference | Notes |
|-----------------|-----------------------|-----------|---|
| 0000::/8 | Reserved by IETF | rfc 4291 | [1] [2][3][4][5] |
| 0100::/8 | Reserved by IETF | rfc 4291 | 0100::/64 reserved for Discard-Only Address Block [RFC6666] |
| 0200::/7 | Reserved by IETF | rfc 4048 | Deprecated as of December 2004 [RFC4048]. Formerly an OSI NSAP-mapped prefix set [RFC4548]. |
| 0400::/6 | Reserved by IETF | rfc 4291 | |
| 0800::/5 | Reserved by IETF | rfc 4291 | |
| 1000::/4 | Reserved by IETF | rfc 4291 | |
| 2000::/3 | Global Unicast | rfc 4291 | IANA unicast address assignments are currently limited to the IPv6 unicast address range of 2000::/3 [6][7][8][9][10][11] |
| 4000::/3 | Reserved by IETF | rfc 4291 | |
| 6000::/3 | Reserved by IETF | rfc 4291 | |

| IPv6 Prefix | Allocation | Reference | Notes |
|-------------|----------------------|-----------|--|
| 8000::/3 | Reserved by IETF | rfc 4291 | |
| a000::/3 | Reserved by IETF | rfc 4291 | |
| c000::/3 | Reserved by IETF | rfc 4291 | |
| e000::/4 | Reserved by IETF | rfc 4291 | |
| f000::/5 | Reserved by IETF | rfc 4291 | |
| f800::/6 | Reserved by IETF | rfc 4291 | |
| fc00::/7 | Unique Local Unicast | rfc 4193 | For complete registration details, see [IANA registry iana-ipv6-special-registry]. |
| fe00::/9 | Reserved by IETF | rfc 4291 | |
| fe80::/10 | Link-Scoped Unicast | rfc 4291 | Reserved by protocol. For authoritative registration, see [IANA registry...] |



IPv6

The IANA IPv6 Address Space

(www.iana.org/assignments/ipv6-address-space/ipv6-address-space.xhtml)

| IPv6 Prefix | Allocation | Reference | Notes |
|---------------------------|------------------|--------------------------|---|
| fec0::/10 | Reserved by IETF | rfc 3879 | Deprecated by [RFC3879] in September 2004. Formerly a Site-Local scoped address prefix. |
| ff00::/8 | Multicast | rfc 4291 | IANA assignments from this block are registered in [IANA registry...] |

- [1] [::1/128](#) reserved for [Loopback Address](#) [RFC4291]. Reserved by protocol. [IANA reg].
- [2] [::/128](#) reserved for [Unspecified Address](#) [RFC4291]. Reserved by protocol. [IANA reg].
- [3] [::ffff:0:0/96](#) reserved for IPv4-mapped Address [RFC4291]. Reserved by protocol. [IANA reg].
- [4] [0000::/96](#) **deprecated** by [RFC4291]. Formerly "**IPv4-compatible IPv6 address**" prefix.
- [5] The "Well Known Prefix" [64:ff9b::/96](#) mapping between IPv4 to IPv6 addresses [RFC6052].
- [6] [2001:0000::/23](#) reserved for IETF Protocol Assignments [RFC2928]. For complete [IANA reg]
- [7] [2001:0000::/32](#) reserved for [TEREDO](#) [RFC4380]. [IANA registry [iana-ipv6-special-registry](#)].
- [8] [2001:0002::/48](#) reserved for Benchmarking [RFC5180]. [IANA registry]
- [9] [2001:db8::/32](#) reserved for Documentation [RFC3849]. [IANA reg].
- [10] [2001:10::/28](#) reserved for ORCHID [RFC4843]. [IANA registry [iana-ipv6-special-registry](#)].
- [11] [2002::/16](#) reserved for [6to4](#) [RFC3056]. [IANA registry [iana-ipv6-special-registry](#)].

- Link-Local IPv6 unicast Addresses **fe80::/10** (**1111111010** binario)
L'indirizzo di Link-Local è pensato per essere utilizzato in un singolo link come indirizzo autoconfigurato, per il neighbor discovery o quando non è presente un router.



- Site-Local IPv6 Unicast Addresses **fec0::/10** (**1111111011** binario)
Deprecato. Pensato per essere usato all'interno di un sito senza la necessità di aver assegnato un Global Prefix. Le nuove implementazioni tratteranno questo prefisso come un normale Global Prefix. Le esistenti continueranno ad usarlo come Site-Local.



- Unique Local IPv6 Unicast Addresses **fc00::/7** (**1111110** binario)
 - Prefix** **fc00::/7** prefisso per identificare l'indirizzo **Local IPv6 Unicast Address**;
 - L** **vale 1** quando il prefisso è assegnato localmente. Il valore 0 verrà assegnato successivamente;
 - Global ID** **40-bits**, identificativo globale usato per creare un prefisso globale unico. Sarà generato usando un algoritmo **pseudo-casuale**. Non può essere creato sequenzialmente o utilizzando indirizzi "well-known" assegnati. Questo tipo d'indirizzo non è pensato per essere propagato;
 - Subnet ID** **16-bits**, identificativo della subnet all'interno del sito;
 - Interface ID** **64-bits**, indirizzo dell'interfaccia in notazione **EUI-64 modificata**.



- Global IDs assegnati localmente e autogenerati senza bisogno di un coordinamento centrale e con un'estrema probabilità di essere unici;
- Devono essere generati con un algoritmo pseudo-casuale possibilmente simile a livello globale per garantirne il più possibile l'unicità:
 - 1) Si ottiene il tempo corrente in formato NTP a 64-bit;
 - 2) Si ottiene l'identificativo EUI-64 del sistema utilizzato per calcolare il global ID. Se il sistema non ha un EUI-64 lo si ottiene modificando il MAC address, se non è disponibile un MAC address si utilizza un altro identificativo unico come il numero seriale del sistema;
 - 3) Si concatena il tempo con l'identificativo per ottenere una chiave;
 - 4) Si utilizza la chiave con un algoritmo SHA-1 per ottenere un identificativo di 160 bits;
 - 5) Si usano i 40 bits più significativi dell'identificativo creato come Global ID;
 - 6) Si concatenano fc00::/7, il bit L a 1 e il Global ID appena creato per ottenere il Local IPv6 address prefix.

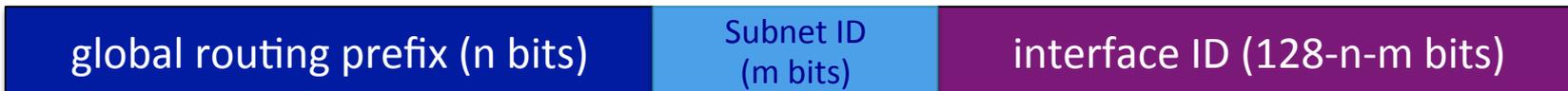
- L'indirizzo IPv6 unicast è aggregabile con prefissi di lunghezza diversa.
- Esistono diversi tipi di indirizzi unicast, Global Unicast, site-local unicast (deprecato), Link-Local unicast e Unique Local Unicast. Esistono alcuni casi speciali del Global Unicast come gli indirizzi IPv6 con inserito l'indirizzo IPv4 e altri che potranno essere definiti in futuro.
- Un indirizzo unicast è rappresentabile dall'unione del prefisso di rete e dall'identificativo dell'interfaccia

subnet prefix (n bits)

interface ID (128-n bits)

- Per gli indirizzi unicast autoconfigurati (stateless) , **l'Interface ID** deve essere lunga **64 bits** e generalmente costruita nel formato **Modified EUI-64** (**Mac OSX e linux**). Può essere costruita utilizzando regole di **privacy** contenute nel **rfc 3041 → 4941** (**MS Windows**)

- **Il formato generale di un indirizzo Global Unicast:** è formato da un prefisso di routing assegnato ad un'Istituzione, da un **Subnet ID** che è l'identificativo di un link interno all'Istituzione e dall'**Interface ID** lunga 64 bits, tranne per gli indirizzi che iniziano col binario 000.



- **IPv4-Compatible IPv6 Address:** è stato definito per permettere l'inserimento di un indirizzo unicast IPv4 nei 32 bit meno significativi dell'indirizzo IPv6. **Deprecato.**(::<192.0.2.1)



- **IPv4-Mapped IPv6 Address:** è stato definito per rappresentare l'indirizzo IPv4 di un nodo come se fosse un indirizzo IPv6 (::ffff:192.0.2.1).



- Nel **rfc6052** (oct 2010) che estende il rfc4291 viene trattato tutto il problema della traduzione da indirizzi IPv6 in IPv4 e viceversa. Viene definito un nuovo prefisso (Well-Known Prefix) **64:ff9b::/96** da utilizzare per gli indirizzi **IPv4-Embedded IPv6 Address** e nuove regole sintattiche per la traduzione utilizzando il **Global Routing Prefix** assegnato. IANA ha aggiunto il nuovo prefisso alle note del prefisso 0000::/8.

| Well-Known Prefix | IPv4 address | IPv4-Embedded IPv6 Address |
|-------------------|--------------|----------------------------|
| 64:ff9b::/96 | 192.0.2.33 | 64:ff9b::192.0.2.33 |

- IPv4-Embedded IPv6 Address** è formato da un prefisso di lunghezza variabile (32, 40, 48, 56, 64, 96), dall'indirizzo IPv4 e da un suffisso di lunghezza variabile. I bits da 64 a 71 sono riservati e sempre a 0.

| Network-Specific Prefix | IPv4 address | IPv4-Embedded IPv6 Address | Encoded Position (bits) |
|-------------------------|--------------|--------------------------------------|-------------------------|
| 2001:db8::/32 | 192.0.2.33 | 2001:db8:c000:221:: | 32-63 (32) |
| 2001:db8:100::/40 | 192.0.2.33 | 2001:db8:1c0:2:21:: | 40-63 (24), 72-79 (8) |
| 2001:db8:122::/48 | 192.0.2.33 | 2001:db8:122:c000:2:2100:: | 48-63 (16), 72-87 (16) |
| 2001:db8:122:300::/56 | 192.0.2.33 | 2001:db8:122:3c0:0:221:: | 56-63(8), 72-95 (24) |
| 2001:db8:122:344::/64 | 192.0.2.33 | 2001:db8:122:344:c0:2:2100:: | 72-103 (32) |
| 2001:db8:122:344::/96 | 192.0.2.33 | 2001:db8:122:344:: 192.0.2.33 | 96-127 (32) |

IPv6 Stateless Autoconfiguration [rfc4291, rfc2464]

- L'interface ID di un'interfaccia Ethernet si basa sull'identificativo EUI-64 ricavato dal MAC address dell'interfaccia (48-bit IEEE 802) e viene formato nel seguente modo:
 - L'OUI dell'indirizzo Ethernet (primi 3 ottetti) diventa il company-id dell'indirizzo EUI-64
 - Il quarto e il quinto ottetto dell'EUI-64 assumono il valore esadecimale **FFFE**
 - Gli ultimi tre ottetti del MAC address diventano gli ultimi tre dell'indirizzo EUI-64
 - In fine viene complementato il "Universal/Local" (U/L) bit che è il secondo bit meno significativo del primo ottetto dell'indirizzo EUI-64. L'Universal bit dell'EUI-64 è 0 mentre un indirizzo unicast IPv6 ha questo bit a 1.
- Un indirizzo Link-Local autonfigurato diventerà:

| | | |
|-------------|--|---------------------------------------|
| MAC address | 00 :1d:60:8b:42:ce | (00000000 primo ottetto) |
| Link-Local | fe80:: 21 d:60: FFFE :8b:42:ce | (00000010 primo ottetto Int.) |

IPv6 Stateless Autoconfiguration [rfc 3041 → 4941]

- Microsoft non usa l'EUI-64 modificato per costruire l'Interface ID dell'indirizzo IPv6:
 - Usa le Privacy extensions per costruire un'Interface ID completamente anonimo anche per l'indirizzo di Link-Local.
 - Affianca all'indirizzo Global Unicast, anche questo anonimo, un indirizzo Global unicast anonimo e temporaneo che varia nel tempo.
 - Usa questo indirizzo temporaneo per tutte le comunicazioni in uscita.
- Mac OSX ha cominciato ad utilizzare le Privacy Extensions dalla versione Lions:
 - Usa L'interface ID EUI-64 modificata per l'indirizzo Link-Local e Global Unicast
 - Affianca un indirizzo temporaneo anonimo che usa per le comunicazioni in uscita
- Linux utilizza l'EUI-64 modificato, alcune distribuzioni hanno introdotto l'uso dell'indirizzo temporaneo:
 - Fedora, Debian e SL solo EUI-64 modificato
 - Ubuntu EUI-64 modificato e indirizzo temporaneo

Windows usa le Privacy Extensions per tutti gli indirizzi Global e Link-Local

MAC **f4:6d:04:d5:9f:1c** (2001:760:2a14:0:**f66d:4ff:fed5:9f1c**)

Global 2001:760:2a14:0:fc75:8ab5:772d:5c5c

Global temp 2001:760:2a14:0:7c4e:aee9:e112:8388

Link-Local fe80::fc75:8ab5:772d:5c5c

```
netsh interface ipv6 set global randomizeidentifiers=disabled
```

Global 2001:760:2a14:0:**f66d:4ff:fed5:9f1c**

Global temp 2001:760:2a14:0:a97d:6178:6e09:4912

Link-Local fe80::**f66d:4ff:fed5:9f1c**

C:\> netsh interface ipv6 (da utilizzare nel prompt dei comandi in modalita ammin.)

Comandi in questo contesto:

- 6to4 - Passa al contesto `netsh interface ipv6 6to4'.
- ? - Visualizza un elenco di comandi.
- add - Aggiunge una voce di configurazione ad una tabella.
- delete - Elimina una voce di configurazione da una tabella.
- dump - Visualizza uno script di configurazione.
- help - Visualizza un elenco di comandi.
- isatap - Passa al contesto `netsh interface ipv6 isatap'.
- reset - Reimposta le configurazioni IP.
- set - Imposta informazioni di configurazione.
- show - Visualizza informazioni.

Sono disponibili i seguenti sottocontesti:

6to4 isatap

Per vedere la guida per un comando, digitare il comando seguito da uno spazio e quindi digitare ?.

Mac OS X (>=Lions) usa le Privacy Extensions per gli Indirizzi temporanei

MAC **28:cf:e9:50:1e:71** (2001:760:2a14:0:**2acf:e9ff:fe50:1e71**)

Global 2001:760:2a14:fffe:**2acf:e9ff:fe50:1e71**

Global temp 2001:760:2a14:fffe:e802:526d:6581:878b

Link-Local fe80::**2acf:e9ff:fe50:1e71**

Per disattivare/attivare l'utilizzo degli indirizzi temporanei si utilizza il comando **sysctl**:

```
$ sysctl -w net.inet6.ip6.use_tempaddr=0      [0=disattiva | 1=attiva]
```

```
$ sysctl -w net.inet6.ip6.prefer_tempaddr=0      [0=disattiva | 1=attiva]
```

Per rendere persistenti le modifiche inserire le variabili (sysctl_mib=value) nel file **/etc/sysctl.conf** (il file non esiste e va creato).

In Mavericks non è più possibile disabilitare completamente l'uso di IPv6 da "System Preferences → Network", il sistema prevede al minimo la presenza dell'indirizzo di Link-Local (fe80::EUI64-Local).

È comunque possibile spegnere completamente IPv6 utilizzando i comandi:

```
$ ipconfig set interface-name NONE-V6 (disabilita IPv6)
```

```
$ ipconfig set interface-name AUTOMATIC-V6 (abilita IPv6)
```

Altri comandi utili per analizzare o modificare le configurazioni di IPv6:

ndp (control/diagnose IPv6 neighbor discovery protocol)

netstat (show network status es.)

ifconfig

linux (tranne ubuntu) non usa le Privacy Extensions per gli Indirizzi temporanei
Per mostrare/disattivare/attivare i parametri del kernel che gestiscono la configurazione di IPv6 si utilizza il comando **sysctl**:

```
$ sysctl -a | grep ipv6 (mostra la configurazione dei parametri)
```

```
$ sysctl -w net.ipv6.conf.[default|all|eth0].use_tempaddr=X
```

dove **X** vale [**0**=disattiva | **1**=attiva | **2**= attiva e preferisci]

Per rendere persistenti le modifiche inserire le variabili (sysctl_mib=value) nel file **/etc/sysctl.conf**

In linux è possibile utilizzare anche il file di configurazione delle interfacce di rete per impostare i parametri IPv6:

Debian (/etc/networks/interfaces)

```
iface eth0 inet6 auto
    privext 2
    dhcp 1
```

(**Attenzione**: riscrive /etc/resolv.conf con le sole informazioni IPv6)

RedHat (/etc/sysconfig/network-scripts/ifcfg-eth0)

```
IPV6_PRIVACY="rfc3041"
```

```
IPV6_PEERDNS="yes" (Attenzione: funziona solo con NetworkManager attivo)
```

- Un IPv6 Anycast Address è un identificativo assegnato ad un gruppo d'interfacce (tipicamente appartenenti a nodi diversi). Un pacchetto inviato ad un indirizzo anycast è consegnato **ad una delle interfacce** contrassegnate da questo indirizzo, la più vicina secondo la misura di distanza del protocollo di routing.
- Gli indirizzi anycast sono allocati nello spazio assegnato agli indirizzi unicast e la loro sintassi è indistinguibile da questi. Quando un indirizzo unicast è assegnato a più d'una interfaccia diventa un indirizzo anycast, i nodi dove questi indirizzi sono assegnati devono essere configurati per riconoscerli come indirizzi anycast.
- Per ogni indirizzo anycast assegnato, esiste una parte dell'indirizzo P che specifica topologicamente la regione dove le interfacce che appartengono dall'indirizzo risiedono. Nella regione identificata da P, l'indirizzo anycast è mantenuto come una entry separata nelle tabelle di routing (host route). Fuori dalla regione identificata da P le informazioni di routing sono aggregate a quelle per il prefisso P.
- Nel peggiore dei casi il prefisso P è nullo, non avendo i membri dell'indirizzo anycast una località topologica. In questo caso le informazioni di routing sono mantenute in entries separate e appartenenti all'intero Internet, la loro scalabilità è enormemente limitata e il supporto per questi indirizzi anycast "globali" può risultare inesistente o veramente ristretto.

- Uno dei possibili usi di questo tipo d'indirizzamento potrebbe essere l'identificazione di tutti i routers appartenenti ad una organizzazione che fornisce il servizio Internet.
- L'indirizzo può essere usato come indirizzo intermedio in un Routing header IPv6 in modo che il pacchetto sia ricevuto attraverso un particolare service provider o attraverso una sequenza di service providers.
- Altri possibili usi sono l'identificazione del set di routers collegati ad un particolare subnet, o il set di routers che garantiscono l'ingresso in un particolare dominio di routing.
- L'utilizzo implementato sembra essere quello dei master server DNS per permetterne una migliore distribuzione e raggiungibilità geografica.

- Subnet-Router Anycast Address: tutti i router devono supportare questo tipo d'indirizzo per tutte le sottoreti configurate.
- La sintassi di questo tipo d'indirizzo è identica ad un qualsiasi indirizzo unicast con l'identificativo d'interfaccia inizializzato a zero.
- Un pacchetto inviato alla Subnet-Router sarà trattato da uno dei routers della sottorete.
- Questo indirizzo è pensato per essere usato da applicazioni che necessitano di comunicare con uno qualsiasi dei routers presenti.

subnet prefix (n bits)

00000000000000 (128-n bits)

IPv6 Reserved Sub-Net Anycast Addresses [rfc2526]

| Decimale | Esadecimale | Descrizione |
|----------|-------------|--|
| 127 | 0x7f | Riservato |
| 126 | 0x7e | Mobile IPv6 Home-Agents anycast (vedi anche rfc3775) |
| 125 | 0x7d | IPv6 Over GeoNetworking geographic anycast (ETSI EN 302 636-6-1) |
| 1-124 | 0x01-0x7c | Riservato |

(<http://www.iana.org/assignments/ipv6-anycast-addresses/ipv6-anycast-addresses.xhtml>)

In ogni subnet gli ultimi bits sono riservati e formano il reserved subnet anycast addresses. Per identificativi d'interfaccia di 64 bits il bit (U/L) è posto a 0 mentre per tutti gli altri l'identificativo d'interfaccia è formato da tutti 1 più i 7 bits dell'Anycast ID.

| | | |
|----------------------|----------------------------------|------------|
| Sub-Net ID (64 bits) | 11111101... (57 bits) ...111111 | Anycast ID |
| Sub-Net ID (n bits) | 111111... (121-n bits) ...111111 | 7 bits |

- Un indirizzo multicast IPv6 è assegnato ad un gruppo d'interfacce solitamente appartenenti a nodi diversi. Un interfaccia può appartenere a diversi gruppi multicast.



ff (11111111 binario) all'inizio dell'indirizzo lo identifica come un indirizzo multicast;

flgs è un set di quattro flags: **0 R T P**

il bit più significativo è riservato e sempre **0**

T = 0 indica un indirizzo permanentemente assegnato ("well-known") da IANA

T = 1 indica un indirizzo non permanente (assegnato come temporaneo o dinamico)

P (rfc3306)

R (rfc3956)

11111111

flgs

scop

Group ID

scop

4 bits multicast scope, serve per limitare lo scopo del gruppo multicast. I valori sono riportati nella tabella:

| Val | Scopo | Val | Scopo |
|-----|------------------------|-----|---------------------------|
| 0 | riservato | 8 | Organization-Local |
| 1 | Interface-Local | 9 | (non assegnato) |
| 2 | Link-Local | a | (non assegnato) |
| 3 | riservato | b | (non assegnato) |
| 4 | Admin-Local | c | (non assegnato) |
| 5 | Site-Local | d | (non assegnato) |
| 6 | (non assegnato) | e | Global |
| 7 | (non assegnato) | f | riservato |

- **Interface-Local:** condivide una singola interfaccia in un nodo ed è usato solo per la trasmissione di multicast in loopback;
- **Link-Local:** condivide la stessa regione topologica del corrispondente scopo unicast;
- **Admin-Local:** è il minor scopo che può essere amministrato,?????
- **Site-Local:** condivide un singolo sito;
- **Organization-Local:** condivide i siti appartenenti ad un'unica Organizzazione;
- (non assegnato) è a disposizione degli amministratori per definire regioni multicast addizionali;
(<http://www.iana.org/assignments/ipv6-multicast-addresses/ipv6-multicast-addresses.xml>)

11111111

ORTP

scop

Group ID

Group ID

I 112 bits identificano il gruppo multicast, sia permanente che temporaneo all'interno dello scopo definito. Vedi anche rfc3306.

- Il significato di indirizzo multicast assegnato in modo permanente è indipendente dal suo scopo. Per esempio, se al “gruppo NTP servers” assegnamo un Group ID 0x101 allora:
 - ff01::101** significa tutti gli NTP servers nella stessa interfaccia di chi invia il pacchetto;
 - ff02::101** significa tutti gli NTP servers nello stesso link di chi invia il pacchetto;
 - ff05::101** significa tutti gli NTP servers nello stesso sito di chi invia il pacchetto;
 - ff0e::101** significa tutti gli NTP servers presenti in Internet.
- Gli indirizzi non permanenti (T = 1) hanno invece significato solo all'interno dello scopo assegnato e non hanno nessuna relazione con gli stessi indirizzi assegnati con scopi diversi o con gli stessi indirizzi assegnati in modo permanente.

- Un indirizzo multicast non può essere usato come indirizzo sorgente in un pacchetto IPv6 o comparire in un Routing header;
- Un router non può propagare un pacchetto multicast al di fuori dello scopo indicato dal campo scop nell'indirizzo multicast di destinazione;
- Un nodo non può originare un pacchetto con un indirizzo multicast che contiene **0** nel campo **scop**; se un pacchetto di questo tipo viene ricevuto deve essere **scartato**.
- Un nodo non può originare un pacchetto con un indirizzo multicast che contiene **f** nel campo **scop**; se un pacchetto di questo tipo viene ricevuto o inviato, deve essere trattato come un pacchetto destinato ad un indirizzo multicast Globale (**scop = e**).

- Gli indirizzi multicast “well-known” che seguono sono predefiniti. I Group IDs definiti in questa sezione hanno uno scopo con un esplicito valore.
- L'utilizzo di questi Group IDs con uno scopo diverso da quello definito, con T = 0, è vietato.

Indirizzi multicast riservati, non possono essere assegnati a nessun gruppo multicast:

**ff00::, ff01::, ff02::, ff03::, ff04::, ff05::, ff06::, ff07::,
ff08::, ff09::, ff0a::, ff0b::, ff0c::, ff0d::, ff0e::, ff0f::**

Indirizzi multicast **All-Nodes**, identificano il gruppo di tutti i nodi IPv6 con scopo 1 (interface-local) e 2 (link-local): **ff01::1, ff02::1**

Indirizzi multicast **All-Routers**, identificano il gruppo di tutti i Routers IPv6 con scopo 1 (interface-local), 2 (link-local) e 5 (site-local): **ff01::2, ff02::2, ff05::2**

Indirizzo **Solicited-node**: **ff02::1:ffxx:xxx**

L'indirizzo multicast Solicited-node è calcolato come funzione dell'indirizzo unicast e anycast del nodo. L'indirizzo è formato prendendo i **24 bits meno significativi** dell'indirizzo unicast o anycast e appendendoli al prefisso multicast **ff02::1:ff00:0/104** ottenendo un indirizzo **tra ff02::1:ff00:0 e ff02::1:ffff:fff**.

Se prendiamo l'indirizzo unicast o anycast di un nodo: **4037::1:800:200e:8c6c** l'indirizzo Solicited-node sarà **ff02::1:ff0e:8c6c**

Indirizzi IPv6 che differiscono solo nella parte più significativa avranno lo stesso indirizzo multicast Solicited-node identico, riducendo così gli indirizzi multicast che un nodo condivide.

Un nodo deve calcolare e associare gli indirizzi multicast Solicited-node per tutti gli indirizzi unicast o anycast configurati nelle proprie interfacce.

(<http://www.iana.org/assignments/ipv6-multicast-addresses/ipv6-multicast-addresses.xml>)

Lista degli indirizzi multicast (**linux**): **ip -6 maddr show**

1: lo

inet6 ff02::1 *(All Nodes Link-Local)*

inet6 ff01::1 *(All Nodes Interface-Local)*

2: em1

inet6 ff02::1:ff**07:d3b8** *(Solicited-node prefix:e925:2faa:99**07:d3b8**)*

inet6 ff02::1:ff**8b:42ce** users 2 *(Solicited-node prefix:21d:60ff:fe**8b:42ce**)*

inet6 ff02::1

inet6 ff01::1

Lista degli indirizzi multicast (**linux, Mac OSX**): **netstat -g -f inet6**

Lista degli indirizzi multicast(**Windows**): **netsh interface ipv6 show joins**

- È richiesto che un **host** riconosca i seguenti indirizzi che lo identificano:
 - l'indirizzo Link-Local per ogni interfaccia;
 - tutti gli indirizzi unicast e anycast aggiuntivi configurati automaticamente o manualmente nelle sue interfacce;
 - l'indirizzo di loopback;
 - gli indirizzi multicast All-Node;
 - gli indirizzi multicast Solicited-Node per tutti gli indirizzi unicast o anycast configurati;
 - Tutti gli indirizzi multicast dei gruppi a cui il nodo appartiene;
- È richiesto che un **Router** riconosca tutti gli indirizzi richiesti per l'host più gli indirizzi specifici che lo identificano:
 - L'indirizzo anycast Subnet-Router per tutte le interfacce per cui fa routing;
 - Tutti gli altri indirizzi anycast per cui il router è configurato;
 - Gli indirizzi multicast All-Routers.

- ~~1885~~ → ~~2463~~ → 4443 (tools.ietf.org/html/rfc4861)

Dec 1995

Dec 1998

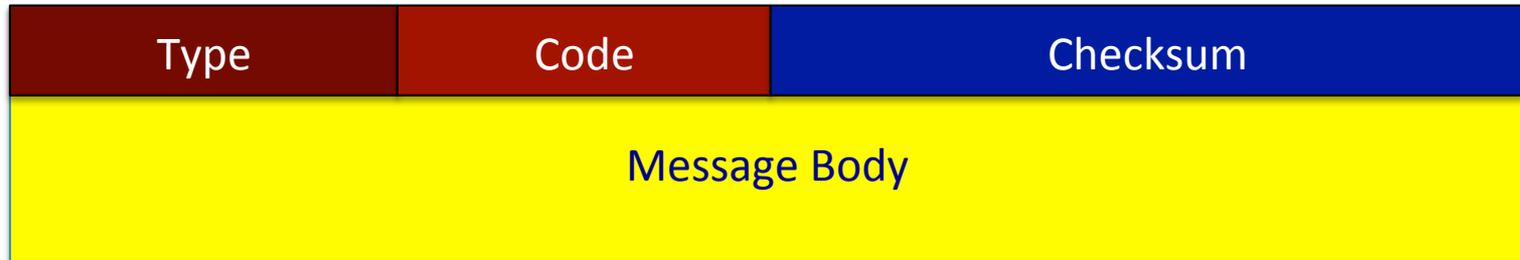
Mar 2006

è uno Standards Track ed è stato aggiornato da:

rfc 4884 ([Apr 2007](#)) Estensione ICMP per il supporto dei messaggi Multi-Part

I messaggi ICMPv6 (Internet Message Control Protocol) sono usati per segnalare errori nel processo dei pacchetti, o per altre funzioni come la diagnostica (ICMPv6 “ping”) e l’invio di messaggi di Neighbor Discovery. ICMPv6 è parte integrale di IPv6, e le specifiche di base del protocollo (quelle che fanno parte di questa specifica) devono essere pienamente implementate da qualsiasi nodo IPv6.

- Ogni messaggio ICMPv6 è preceduto da un header IPv6 e da zero o più **extension headers** IPv6. L'header ICMPv6 è identificato dal valore **58** del campo Next header dell'header che lo precede.
Type: 8-bits indica il tipo di messaggio, dal suo valore dipende il formato dei restanti dati. I valori da **0 a 127** indicano messaggi d'**errore**, da **128 a 255** messaggi **informativi**;
Code: 8-bits il suo valore dipende dal tipo, serve per creare un maggiore livello di granularità dei messaggi;
Checksum: 16-bits serve per controllare che il messaggio sia integro.



- ~~1970~~ → ~~2461~~ → 4861 (tools.ietf.org/html/rfc4861)

Aug 1996

Dec 1998

Sep 2007

è uno Standards Track ed è stato aggiornato da:

rfc 5942 (Jul 2010) Rapporto tra i link e i prefissi di subnet

rfc 6980 (Aug 2013) Implicazioni di sicurezza nella frammentazione con ND

rfc 7136 (Jan 2014) Troppo impaziente la rilevazione della Neighbor Unreachability

Questo protocollo risolve una serie di problemi legati all'interazione tra nodi sullo stesso link. Definisce meccanismi per risolvere i seguenti problemi:

- **Router discovery:** come un host scopre i routers collegati allo stesso link;
- **Prefix discovery:** come un host scopre tutti i prefissi degli indirizzi che indicano quali destinazioni sono raggiungibili per un link collegato. (I Nodi usano i prefissi per distinguere quali destinazioni sono on-link da quelle raggiungibili solo attraverso un router).
- **Parameter discovery:** come un nodo impara certi parametri del link come la MTU, o parametri Internet come il valore dell'hop limit da inserire nei pacchetti in uscita.
- **Address autoconfiguration:** introduce il meccanismo che permette agli hosts di configurare un indirizzo per una interfaccia in modo stateless.

- **Address resolution:** come un nodo scopre l'indirizzo link-layer di un dispositivo on-link (es. neighbor) fornendo solo l'indirizzo di destinazione.
- **Next-hop determination:** l'algoritmo per mappare l'indirizzo di una destinazione IP nell'indirizzo del neighbor, al quale il traffico deve essere indirizzato per raggiungere la destinazione finale. Il next-hop può essere un router o la stessa destinazione.
- **Neighbor Unreachability Detection:** come un nodo stabilisce che un neighbor non è più raggiungibile. Per i neighbor usati come router viene tentata una default destination alternativa. Sia per i routers che per gli hosts viene ripetuto l'Address resolution.
- **Duplicate address detection:** come un nodo scopre se l'indirizzo che vorrebbe usare è già in uso.

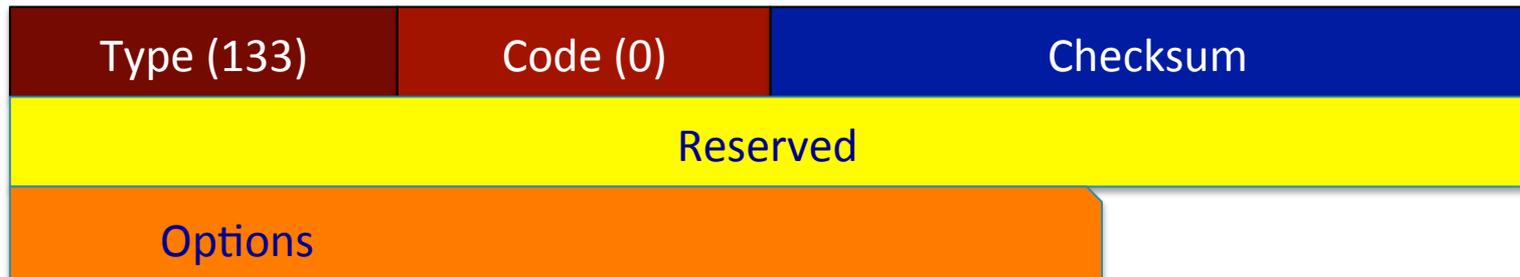
- **Redirect:** come un router informa un host del migliore first-hop per raggiungere una destinazione. Questo meccanismo permette lo scambio di pacchetti tra hosts con indirizzi diversi, ma sullo stesso link, senza doversi inviare i pacchetti attraverso il router.

Neighbor Discovery definisce cinque nuovi messaggi ICMPv6:

- **Router Solicitation:** quando un'interfaccia diventa attiva l'host invia immediatamente un messaggio di Router Solicitation per richiedere al router di generare immediatamente un messaggio di Router Advertisement senza attendere il successivo invio schedulato.
- **Router Advertisement:** i routers avvisano della loro presenza ad intervalli stabiliti o in risposta ad un messaggio di Router Solicitation. I messaggi di Router Advertisement contengono i prefissi che vengono usati per definire se un altro indirizzo condivide lo stesso link (on-link determination) e/o per la configurazione dell'indirizzo, il valore dell'hop-limit consigliato etc.

- **Neighbor Solicitation:** inviato da un nodo per determinare l'indirizzo di link-layer di un neighbor o per stabilire se un neighbor è ancora raggiungibile attraverso il link-layer registrato nella cache. Il messaggio di neighbor Solicitation è usato anche per la Duplicate Address Detection.
- **Neighbor Advertisement:** risposta ad un messaggio di Neighbor Solicitation. Un nodo può inviare una unsolicited Neighbor Advertisement per comunicare il cambio dell'indirizzo di link-layer.
- **Redirect:** messaggio usato dal router per informare l'host del miglior first-hop per una destinazione.

- **Router Solicitation Message Format:** un host invia un messaggio di Router Solicitation per richiedere al router di inviare un Router Advertisement.



IP fields:

Source Address: un indirizzo IP dell'interfaccia sorgente, o l'indirizzo unspecified se l'interfaccia non ha ancora l'indirizzo;

Destination Address: solitamente l'indirizzo multicast all-routers ff02::2

Hop Limit: 255

ICMP fields:

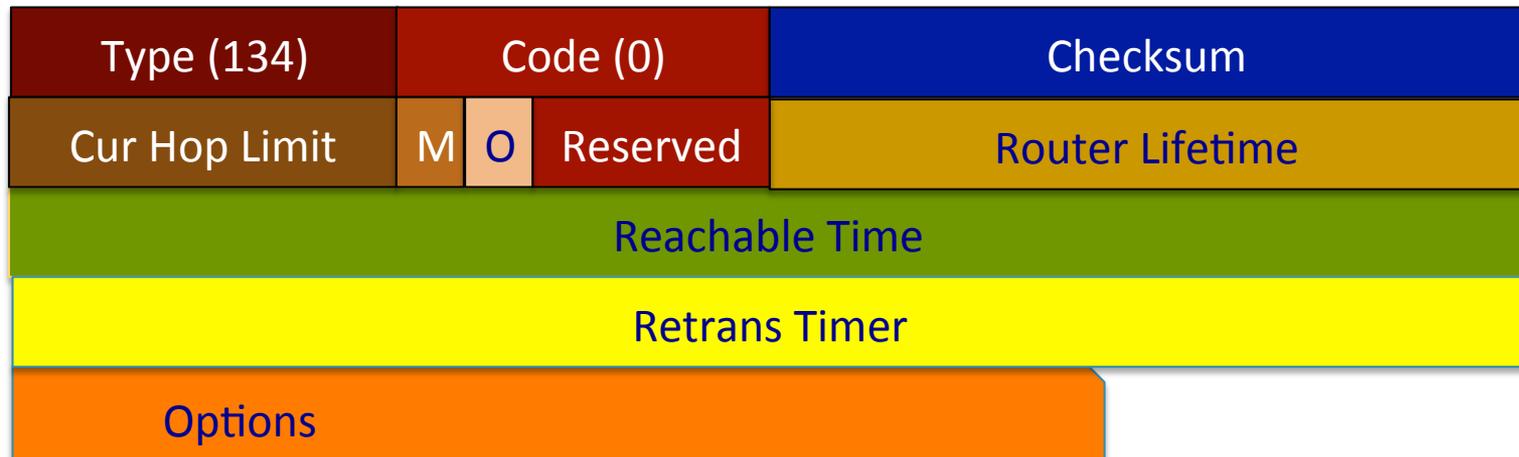
| | |
|-----------------|--|
| Type | 133 |
| Code | 0 |
| Checksum | il checksum ICMP. |
| Reserved | Campo inutilizzato. Deve essere inizializzato a 0 da chi invia e ignorato da chi riceve. |

Valid Options:

Source link-layer address L'indirizzo di link-layer di chi invia, se conosciuto. Non deve essere specificato se sconosciuto.

Future versioni del protocollo possono definire nuove opzioni. Chi riceve deve scartare le opzioni che non conosce e continuare a processare il messaggio.

- **Router Advertisement Message Format:** un Router invia un messaggio di Router Advertisement periodicamente o in risposta ad un messaggio di Router Solicitations.



IP fields:

Source Address

l'indirizzo di link-local assegnato all'interfaccia dalla quale è stato spedito il messaggio

Destination Address

solitamente l'indirizzo sorgente di chi ha invocato la Router Solicitation o l'indirizzo multicast di all-nodes ff02::1

Hop Limit 255

ICMP fields:

| | |
|----------------------|---|
| Type | 134 |
| Code | 0 |
| Checksum | il checksum ICMP. |
| Cur Hop Limit | 8-bit unsigned integer. Il valore di default che deve essere inserito nel campo Hop Count dell'header IP dei pacchetti da inviare. |
| M | 1-bit. Flag di "Managed address configuration". Se settato indica che l'indirizzo è disponibile via DHCPv6. |
| O | 1-bit. Flag di "Other configuration" Se settato indica che altre configurazioni sono disponibili via DHCPv6. solitamente si tratta di informazioni relative al DNS. |

Nota: se ne M ne O sono settati significa che nessuna informazione è disponibile via DHCPv6.

ICMP fields:

Reserved

6-bit. Campo inutilizzato. Deve essere inizializzato a 0 da chi invia e ignorato da chi riceve.

Router Lifetime

16-bit unsigned integer. Il lifetime associato al default router in secondi. Un lifetime di 0 indica che il router non è un default router e non deve essere inserito nella lista dei default routers. Il lifetime si applica solo ai default routers.

Reachable Time

32-bit unsigned integer. Il tempo in millisecondi che un nodo usa per considerare un neighbor raggiungibile, dopo aver ricevuto conferma della sua raggiungibilità. Usato dall'algoritmo Neighbor Unreachability Detection. Se 0 non è specificato da questo router.

ICMP fields:

Retrans Timer

32-bit unsigned integer. Tempo in millisecondi prima della ritrasmissione di un messaggio di Neighbor Solicitation. Usato Dall'algoritmo di address resolution e NUD. Se vale 0 non è specificato da questo router.

Possibili Opzioni:

Source link-layer

indirizzo di link-layer dell'interfaccia dalla quale è inviato il messaggio di Router Advertisement. Usato solo nei link layers che hanno un indirizzo. Un Router può omettere questa opzione per abilitare in ingresso il load sharing tra indirizzi multipli di link-layer.

MTU

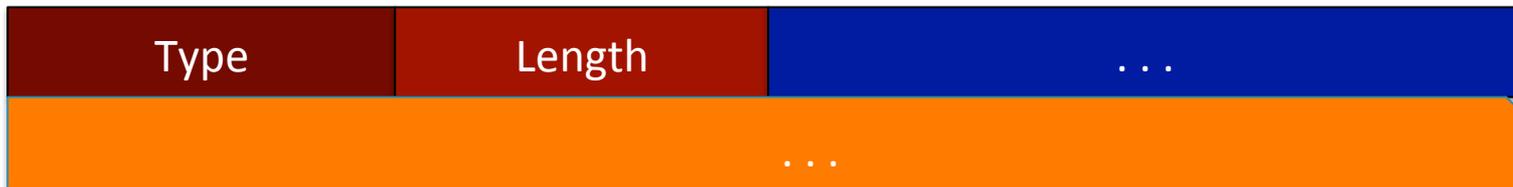
Deve essere inviato in links che hanno una MTU variabile. Può essere inviato in altri links.

Possibili Opzioni:

Prefix Information

Questa opzione specifica i prefissi che sono on-link e possono essere usati per la stateless address autoconfiguration. Un router deve includere tutti i suoi prefissi on-link in modo che i multihomed hosts abbiano la completa informazione sulle destinazioni on-link per i links a cui sono connessi. Se l'informazione è incompleta, un host con più interfacce non sarà in grado di scegliere l'interfaccia di uscita per il traffico spedito ai suoi neighbors.

Formato delle Opzioni



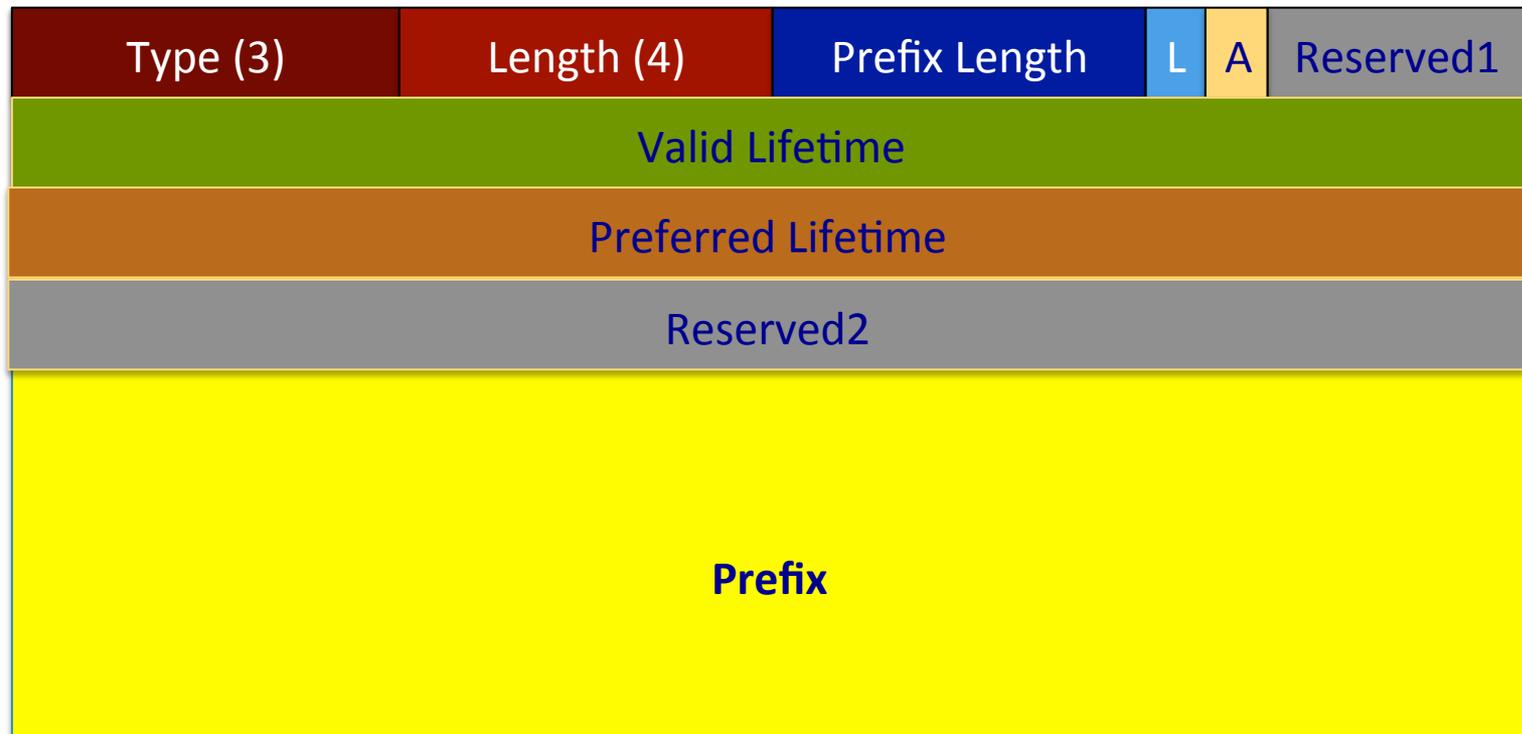
Option fields:

Type 8-bit. Identificativo del tipo d'opzione:

- Source Link-Layer address 1
- Target Link-Layer address 2
- Prefix Information 3
- Redirected Header 4
- MTU 5

Length 8-bit unsigned integer. La lunghezza dell'opzione (incluso il campo Type e Length) in unità di 8 ottetti. Il valore 0 non è valido. I nodi devono scartare un pacchetto ND che contiene un'opzione di lunghezza 0.

Prefix Information



Prefix fields:

- Prefix Length** 8-bit unsigned integer. Il numero dei bit nel prefisso che sono validi. Il valore è tra 0 e 128. Questo campo contiene le informazioni necessarie per decidere la posizione on-link (quando viene combinato con il flag L). Assiste l'autoconfigurazione dell'indirizzo, per cui il valore del campo ha diverse restrizioni.
- L** 1-bit on-link flag. Quando settato indica che un host è on-link se non settato NON significa che l'host è off-link.
- A** 1-bit autonomous address-configuration flag. Quando settato indica che il prefisso può essere usato per la configurazione stateless.

Prefix fields:

Reserved1 6-bit non utilizzati. Deve essere settato a 0 da chi invia e ignorato da chi riceve.

Valid Lifetime 32-bit unsigned integer. Tempo in secondi (dall'invio del pacchetto) di validità del prefisso per la determinazione dell'on-link. Il valore a 1 di tutti i bit (0xffffffff) rappresenta un tempo infinito. Il campo è usato anche dalla configurazione dell'indirizzo.

Preferred Lifetime 32-bit unsigned integer. Tempo in secondi (dall'invio del pacchetto) nel quale l'indirizzo autoconfigurato rimane preferito. Il valore a 1 di tutti i bit (0xffffffff) rappresenta un tempo infinito. Questo tempo non può essere maggiore del valore di Valid Lifetime.

Prefix fields:

Reserved2

campo non utilizzato. Deve essere settato a 0 da chi invia e ignorato da chi riceve.

Prefix

Un indirizzo IP o un prefisso di un indirizzo IP. Il campo Prefix Length contiene il numero di bits validi. I bits nel prefisso che eccedono il prefix length devono essere settati a 0 da chi invia e ignorati da chi riceve. Un router NON può inviare un prefisso di Link-Local e l'host lo deve ignorare se lo riceve.

L'informazione del prefisso fornisce all'host i prefissi on-link e i prefissi per l'autoconfigurazione dell'indirizzo. L'opzione di Prefix Information è fornita dal pacchetto di Router Advertisement e deve essere ignorata se presente in altri messaggi.

Come funziona l'invio di un pacchetto:

- L'host che invia usa una combinazione di informazioni presenti nella [Destination Cache](#), [Prefix List](#) e [Default Router List](#) per determinare l'indirizzo IP dell'appropriato next-hop ([next-hop determination](#)). Se l'indirizzo IP del next-hop è conosciuto viene consultata la [Neighbor Cache](#) per recuperare le informazioni di [link-layer](#).
- La determinazione del next-hop avviene confrontando il prefisso con quelli contenuti nella Prefix List, per decidere se la destinazione è on-link o off-link. Se on-link l'indirizzo del next-hop sarà identico alla destinazione, se off-link verrà scelto l'appropriato router dalla [Default Router List](#).
- La next-hop determination non viene compiuta per ogni pacchetto inviato. L'indirizzo di next-hop, una volta conosciuto, viene salvato nella [Destination Cache](#) (questa contiene anche gli aggiornamenti estratti dai messaggi di Redirect). Se l'indirizzo di next-hop è sconosciuto viene invocata la next-hop determination.
- Quando un indirizzo di next-hop è noto viene consultata la [Neighbor Cache](#) per le informazioni di link-layer del destinatario. Se non esistono informazioni, chi invia inizia l'[Address Resolution](#) e mette in coda il pacchetto aspettandone la risoluzione. Nelle interfacce che gestiscono il [multicast](#) l'Address Resolution consiste nell'inviare un pacchetto di [Neighbor Solicitation](#) e nel ricevere un pacchetto di [Neighbor Advertisement](#), l'informazione ricevuta verrà poi inserita nella [Neighbor Cache](#) e il pacchetto inviato.

- Il GARR ha assegnato a INAF il prefisso:

2001:760:2a00::/40

2⁸ (256) prefissi /48 da **2001:760:2a00::/48** a **2001:760:2aff::/48**

2¹⁶ (65.536) prefissi /64 ogni prefisso /48

2⁶⁴ (18446744073709551616) interfaccie ogni prefisso /64

IPv6 IPv6: i prefissi assegnati alle strutture INAF

| Prefisso | Struttura | Prefisso | Struttura |
|--------------------|-----------------------------|--------------------|--------------------|
| 2001:760:2a00::/48 | Roma Presidenza | 2001:760:2a01::/48 | OA Arcetri (FI) |
| 2001:760:2a02::/48 | OA Bologna | 2001:760:2a03::/48 | OA Capoterra (CA) |
| 2001:760:2a04::/48 | OA Catania | 2001:760:2a05::/48 | OA Collurania (TE) |
| 2001:760:2a06::/48 | OA Brera (MI) | 2001:760:2a07::/48 | OA Merate (LC) |
| 2001:760:2a08::/48 | OA Monte Porzio Catone (RM) | 2001:760:2a09::/48 | OA Napoli |
| 2001:760:2a0a::/48 | OA Padova | 2001:760:2a0b::/48 | OA Palermo |
| 2001:760:2a0c::/48 | OA Torino | 2001:760:2a0d::/48 | OA Trieste |
| 2001:760:2a0e::/48 | IAPS (RM) | 2001:760:2a0f::/48 | |
| 2001:760:2a10::/48 | | 2001:760:2a11::/48 | IASF (MI) |
| 2001:760:2a12::/48 | IASF (PA) | 2001:760:2a13::/48 | IASF (BO) |
| 2001:760:2a14::/48 | IRA (BO) | 2001:760:2a15::/48 | Medicina (BO) |
| 2001:760:2a16::/48 | eVLBI Medicina (BO) | 2001:760:2a17::/48 | Noto (SR) |
| 2001:760:2a18::/48 | S. Basilio (CA) | | |

- **linux (Debian)**, i comandi e i files di configurazione per il **server**:
 - **/usr/sbin/radvd** Router Advertisement Daemon
 - **/etc/radvd.conf** file di configurazione per il daemon radvd
 - **/etc/network/interfaces** file di configurazione delle interfacce ethernet
 - **/etc/sysctl.conf** file di controllo dei parametri del kernel
 - **/usr/sbin/named** DNS server daemon
 - **/etc/bind/*** files per la configurazione del daemon DNS e delle zone
 - **/usr/sbin/apache2** HTTPD server daemon
 - **/etc/apache2/*** files di configurazione del daemon HTTPD

- **/etc/network/interfaces:**

```
# The loopback network interface
auto lo
iface lo inet loopback
# The primary network interface
allow-hotplug eth0
iface eth0 inet static
    address 192.168.77.11
    netmask 255.255.255.0
    gateway 192.168.77.1
    dns-nameservers 192.168.77.11
    dns-search ipv6.inaf.it
iface eth0 inet6 static
    address 201:760:24ff:ffff::11/64
    netmask 64
    accept_ra 0
    autoconf 0
```

- **/usr/sbin/radvd** [apt-get install radvd (installa radvd e radvdump)]
- **/usr/etc/radvd.conf**

```
interface eth0
{
    AdvSendAdvert on;
    AdvManagedFlag off;
    AdvOtherConfigFlag on;
    AdvReachableTime 0;
    AdvRetransTimer 0;
    AdvCurHopLimit 64;
    AdvDefaultLifetime 1800;
    AdvHomeAgentFlag off;
    AdvDefaultPreference medium;
    AdvSourceLLAddress on;
    AdvLinkMTU 1500;
```

- **/usr/etc/radvd.conf**

```
prefix 2001:760:2aff:ffff::/64
{
    AdvValidLifetime 2592000;
    AdvPreferredLifetime 604800;
    AdvOnLink on;
    AdvAutonomous on;
    AdvRouterAddr off;
}; # End of prefix definition
```

```
RDNSS 2001:760:2aff:ffff::11
{
}; # End of RDNSS
```

```
DNSSEC ipv6.inaf.it
{
}; # End of DNSSEC
```

```
}; # End of interface definition
```

- **/etc/sysctl.conf** (deve essere abilitato il forwarding di IPv6)

...

```
# Uncomment the next line to enable packet forwarding for IPv6
```

```
# Enabling this option disables Stateless Address Autoconfiguration
```

```
# based on Router Advertisements for this host
```

```
net.ipv6.conf.all.forwarding=1
```

...

Da linea di comando:

```
$ sysctl -w net.ipv6.conf.all.forwarding=1
```

- `/usr/sbin/named` (apt-get install bind9)
- `/etc/bind/named.conf.options`
directory `"/var/cache/bind";`
...
listen-on port 53 { 192.168.77.11; 127.0.0.1; };
listen-on-v6 { **any**; };

- **/etc/bind/named.conf.local**

```
zone "ipv6.inaf.it" IN {  
    type master;  
    file "ipv6.inaf.it.hosts";  
};  
  
zone "77.168.192.in-addr.arpa" IN {  
    type master;  
    file "192.168.77.0.rev";  
};  
  
zone "f.f.f.f.f.a.2.0.6.7.0.1.0.0.2.ip6.arpa"{  
    type master;  
    file "2001.760.2aff.ffff.rev";  
};
```

- **/var/cache/bind/ipv6.inaf.it.hosts**

```
;;
$TTL 86400
;;
@ IN SOA pula.ipv6.inaf.it. postmaster.mail.ipv6.inaf.it. (
    2014091500 ; Serial
    86400      ; Refresh
    1800      ; Retry
    604800    ; Expire
    172800 )   ; Minimum
;;
;; Name servers
@ IN NS pula.ipv6.inaf.it.
;;
;; Mail exchangers
@ IN MX 10 mail.ipv6.inaf.it.
;;
pula 86400 IN A 192.168.77.11
      86400 IN AAAA 2001:760:2aff:ffff::11
mail 86400 IN CNAME pula.ipv6.inaf.it.
www 86400 IN CNAME pula.ipv6.inaf.it.
```

- `/var/cache/bind/192.168.77.0.rev`

```
;;
$TTL 86400
;;
@      IN      SOA     pula.ipv6.inaf.it. postmaster.mail.ipv6.inaf.it. (
                                2014091500   ; Serial
                                86400         ; Refresh
                                1800          ; Retry
                                604800        ; Expire
                                172800 )      ; Minimum

;;
;; Name servers
;;
@              IN      NS      pula.ipv6.inaf.it.
;;
;;
11             86400   IN      PTR   pula.ipv6.inaf.it.
```


\$ host pula

pula.ipv6.inaf.it has address 192.168.77.11

pula.ipv6.inaf.it has IPv6 address 2001:760:2aff:ffff::11

\$host -6 pula

pula.ipv6.inaf.it has address 192.168.77.11

pula.ipv6.inaf.it has IPv6 address 2001:760:2aff:ffff::11

\$ host -6 2001:760:2aff:ffff::11

1.1.0.0.0.0.0.0.0.0.0.0.0.0.0.0.f.f.f.f.f.f.a.2.0.6.7.0.1.0.0.2.**ip6.arpa** domain
name pointer **pula.ipv6.inaf.it**.

- `/usr/sbin/apache2` [apt-get install apache2]
- `/usr/etc/apache2/*`

apache (httpd) non ha bisogno di particolari settaggi per abilitare l'utilizzo di indirizzi IPv6, se l'interfaccia ethernet del server apache ha configurato sia l'indirizzo IPv4 sia l'indirizzo IPv6 il binding della porta 80 è automatico.

Potete controllare che questa condizione sia vera col comando:

```
$ netstat -peanut | grep tcp6
```

```
...
tcp6      0    0 :::80          :::*           LISTEN
0         20442  5207/apache2
tcp6      0    0 :::53          :::*           LISTEN
115      6802  2567/named
tcp6      0    0 :::22          :::*           LISTEN
0         9172  3962/sshd
...
```

- **Mac OSX**, i comandi per il **server**:
 - **rtadvd** Router Advertisement Daemon
- **linux (Debian)**, i comandi per il **client**:
 - **/usr/sbin/rdisc6** ICMPv6 Router Discovery tool (apt-get install rdisc6)
 - **/etc/rdnssd** ICMPv6 Recursive DNS Server discovery Daemon
- **Mac OSX**, i comandi per il **client**:
 - **/sbin/rtsol[d]** ICMPv6 Router Solicitation command[Daemon]

- `/usr/sbin/rdisc6` (`$ rdisc6 eth0`)

Soliciting ff02::2 (ff02::2) on eth0...

(inviato all'indirizzo multicast di link-layer All-Routers)

```
Hop limit           :           64 (  0x40)
Stateful address conf. :           No
Stateful other conf. :           Yes
Router preference   :      medium
Router lifetime     :      1800 (0x00000708) seconds
Reachable time      : unspecified (0x00000000)
Retransmit time     : unspecified (0x00000000)
Prefix              : 2001:760:2aff:ffff::/64
Valid time          :   2592000 (0x00278d00) seconds
Pref. time         :    604800 (0x00093a80) seconds
Recursive DNS server : 2001:760:2aff:ffff::1
DNS server lifetime :           600 (0x00000258) seconds
MTU                 :           1500 bytes (valid)
Source link-layer address : 00:11:D8:70:4B:91
from fe80::211:d8ff:fe70:4b91
```

- In sala è presente un router IPv6 (linux + radvd) che riproduce l'ambiente di test appena descritto. Per verificarne il funzionamento collegate i vostri portatili all'AP Wireless di test:
 - SSID **PulaIPv6**
 - Password **PulaIPv6_Test**
- Riceverete indirizzi IPv6 con prefisso 2001:760:2aff:ffff::/64
- Per provare il **web** con IPv6 usate l'indirizzo IPv6 **[2001:760:2aff:ffff::1]** e poi il nome host **www.ipv6.inaf.it**

- Configurare il routing IPv6 lato LAN, prefissi, advertisement, DHCPv6/RDNSSD per la stateless configuration dei parametri DNS (flag O) e le access-lists se richieste.
- Configurare il DNS master e/o slaves per la risoluzione degli indirizzi IPv6 assegnati ai servers (DNS compresi).
- Inviare una mail di richiesta (vedi esempio) al GARR-NOC e GARR-LIR per richiedere l'indirizzo punto-punto per la WAN e la registrazione del/dei DNS
- Configurare l'indirizzo ricevuto sull'interfaccia che si collega al peer GARR, e configurare il default gateway (::/0) verso l'indirizzo del peer GARR.
- Chiamare il GARR-NOC per l'attivazione e i test.



IPv6

Mail al GARR-NOC e al GARR-LIR

From: Franco Tinarelli <f.tinarelli@ira.inaf.it>

To: noc@garr.it

CC: lir@garr.it, m.nanni@ira.inaf.it (APA di INAF)

Subject: Richiesta di routing IPv6 per IRA-Bologna

Ciao a tutti,

in qualita' di APM dell'Area della Ricerca di Bologna chiedo
l'attivazione del routing ipv6 per il prefisso /48 assegnato all'Istituto IRA
di Bologna:

2001:760:2a14::/48

Responsabile tecnico del prefisso e':

Franco Tinarelli

Istituto IRA

INAF Area della Ricerca di Bologna

Via Gobetti, 101

40129 BOLOGNA (ITALY)

Tel +39 051 6399409

Fax +39 051 6399431

E-mail: f.tinarelli@ira.inaf.it

Si chiede la registrazione al LIR dei seguenti nameserver per la risoluzione inversa:

d1.ira.inaf.it - Master

area.bo.cnr.it – Slave

Si chiede al GARR il servizio di slave nameserver e la conseguente registrazione di:

ns1.garr.net – Slave

Grazie

Franco Tinarelli

```
ip name-server 2001:760:2A14::11 (aggiungere gli indirizzi IPv6 dei DNS)
ip name-server 2A00:1620:A0::13
!
ipv6 unicast-routing (abilitare il routing IPv6 unicast)
!
ipv6 dhcp pool vlan3-ira (creare le informazioni dhcp)
  dns-server 2001:760:2A14::11
  dns-server 2A00:1620:A0::13
  domain-name ira.inaf.it
!
ipv6 multicast-routing (abilitare il multicast-routing)
!
Interface GigabitEthernetX/X
  description >>| POP GARR AdR-BO|<<
  ipv6 address 2001:760:FFFF:110::1/127 (aggiungere il link verso il GARR)
  ipv6 enable
  ipv6 traffic-filter ipv6_in in (attivare le access-lists in ingresso)
  ipv6 nd ra suppress (disattivare l'advertise sulla punto-punto)
```

```
interface Vlan3
  ipv6 address 2001:760:2A14::1/64
  ipv6 enable
  ipv6 nd prefix 2001:760:2A14::/64 no-advertise
  ipv6 nd prefix 2001:760:2A14:FFFE::/64           (prefisso per l'advertisement)
  ipv6 nd other-config-flag                       (abilita il flag O)
  ipv6 dhcp server vlan3-ira                      (indica il server dhcp)
  !
  ipv6 route ::/0 2001:760:FFFF:110::           (default route)
  ipv6 mld snooping                              (ricerca del percorso multicast)
  !
```

```
ipv6 access-list ipv6_in
remark =====Limita ICMPv6
sequence 11 deny icmp any any 100
sequence 12 deny icmp any any 101
sequence 13 deny icmp any any router-renumbering      (138)
sequence 14 deny icmp any any 139
sequence 15 deny icmp any any 140
sequence 16 deny icmp any any 200
sequence 17 deny icmp any any 201
sequence 20 permit icmp any any
```

```
remark ===== Regole per IRA
```

```
sequence 101 permit tcp any 2001:760:2A14::/64 established
```

```
sequence 102 permit tcp any 2001:760:2A14:FFFE::/64 established
```

```
sequence 111 permit tcp any host 2001:760:2A14::11 eq domain
```

```
sequence 112 permit udp any host 2001:760:2A14::11 eq domain
```

```
sequence 121 permit tcp any host 2001:760:2A14::15 eq www
```

```
sequence 122 permit tcp any host 2001:760:2A14::15 eq 443
```

```
sequence 123 permit tcp any host 2001:760:2A14::13 eq www
```

```
sequence 124 permit tcp any host 2001:760:2A14::13 eq 443
```

```
sequence 151 permit tcp any host 2001:760:2A14::13 eq smtp
```

```
sequence 152 permit tcp any host 2001:760:2A14::13 eq 143
```

```
sequence 153 permit tcp any host 2001:760:2A14::13 eq 220
```

```
sequence 154 permit tcp any host 2001:760:2A14::13 eq 587
```

```
sequence 155 permit tcp any host 2001:760:2A14::13 eq 993
```

```
sequence 156 permit tcp any host 2001:760:2A14::13 eq 995
```

```
sequence 157 permit tcp any host 2001:760:2A14::13 range pop2 pop3
```

```
remark ===== Nega tutto
```

```
sequence 4294967294 deny ipv6 any any
```

(Lucidi Compresi!!!!!!!!!!!!!!!!!!!!;-)