Consortium GARR

Tutorial IPv6

Valentino Carcione

Gabriella Paolini

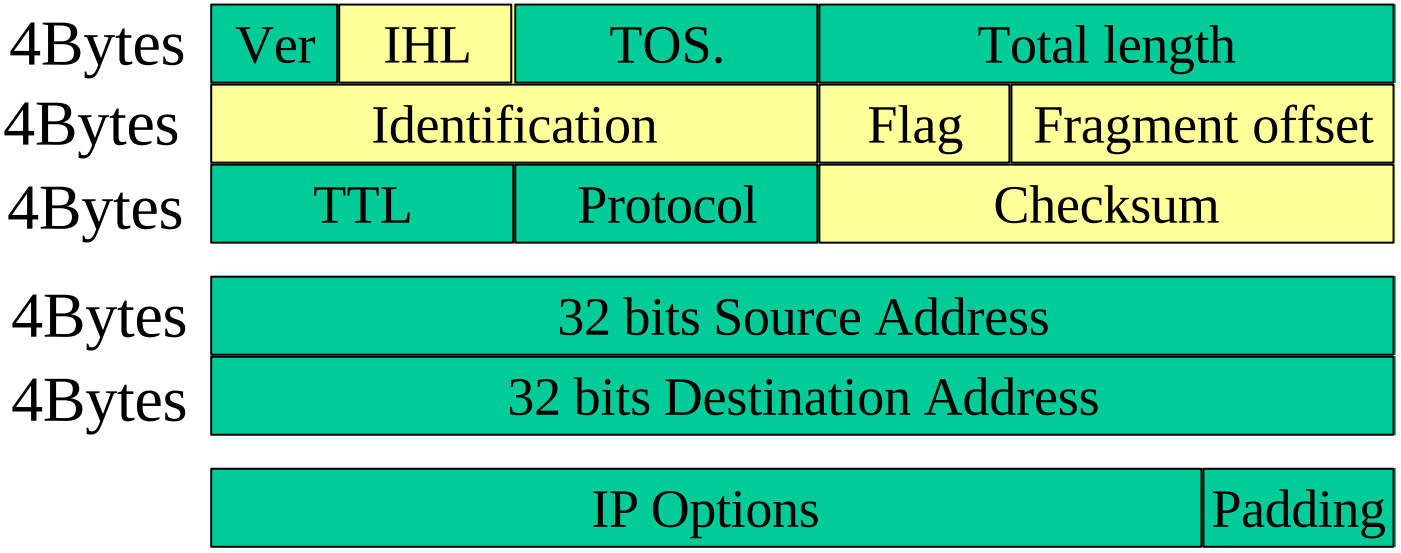
GARR

Consortium GARR

Header IPv6

Header IPv4

– 20 bytes senza il campo options



In giallo i campi che non sono più implementati in IPv6

Header IPv4

- **Version.** 4 bit.
  - Specifica il formato dell'Header del pacchetto IP
  - **4 -** IP, Internet Protocol.
- **IHL, Internet Header Length.** 4 bit.
  - Specifica la lunghezza dell'Header del pacchetto IP in gruppi di 32 bits. Il valore minimo e' 5.
- **TOS, Type of Service.** 8 bit.
  - Specifica i parametri del tipo di servizio richiesto. Questo parametro puo' essere utilizzato per definire la gestione del pacchetto durante il suo trasporto.
- **Total length.** 16 bit.
  - Contiene la lunghezza totale del pacchetto.

Header IPv4

- **Identification.** 16 bit.
  - Usato per identificare il frammento di un pacchetto nel caso sia frammentato.
- **Flags.** 3 bit.
  - Controlla la frammentazione del pacchetto.
- **Fragment Offset.** 13 bit.
  - Usato per ordinare la ricostruzione di un pacchetto frammentato.

Header IPv4

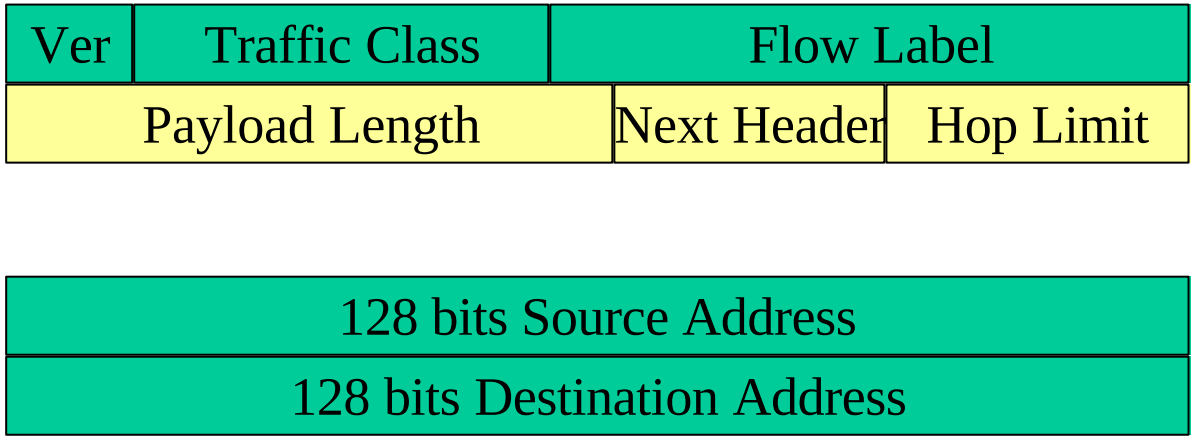
- **TTL, Time to Live.** 8 bit.
  - Un campo timer usato per tracciare il tempo di vita del pacchetto.
- **Protocol.** 8 bit.
  - Specifica il successivo protocollo incapsulato di livello piu' alto.
- **Header checksum.** 16 bit.
  - Checksum dell'header IP incluse le opzioni.

Header IPv4

- **Source IP address.** 32 bit.
  - Indirizzo IP del mittente.
- **Destination IP address.** 32 bit.
  - Indirizzo IP del destinatario.
- **Options.** Lunghezza variabile.
- **Padding.** Lunghezza variabile.
  - Serve per garantire che l'header del pacchetto sia allineata su 32 bit.

Header IPv6

– 40 byte senza le altre header extensions



In giallo i campi ereditati da IPv4 ma rinominati

Header IPv6

- **Version.** 4 bit.
  - **6 -** IPv6.
- **Traffic Class.** 8 bit.
  - Valore per identificare la priorita' del pacchetto nel traffico Internet. (simile al TOS IPv4)
  - Possibili Applicazioni:
    - Differenziazione del traffico immesso nella rete di un ISP da un suo cliente
    - L'ISP può modificare questo campo per tutti i pacchetti in uscita verso altre reti, al fine di assegnare una classe di servizio concordata con altri ISP

Header IPv6

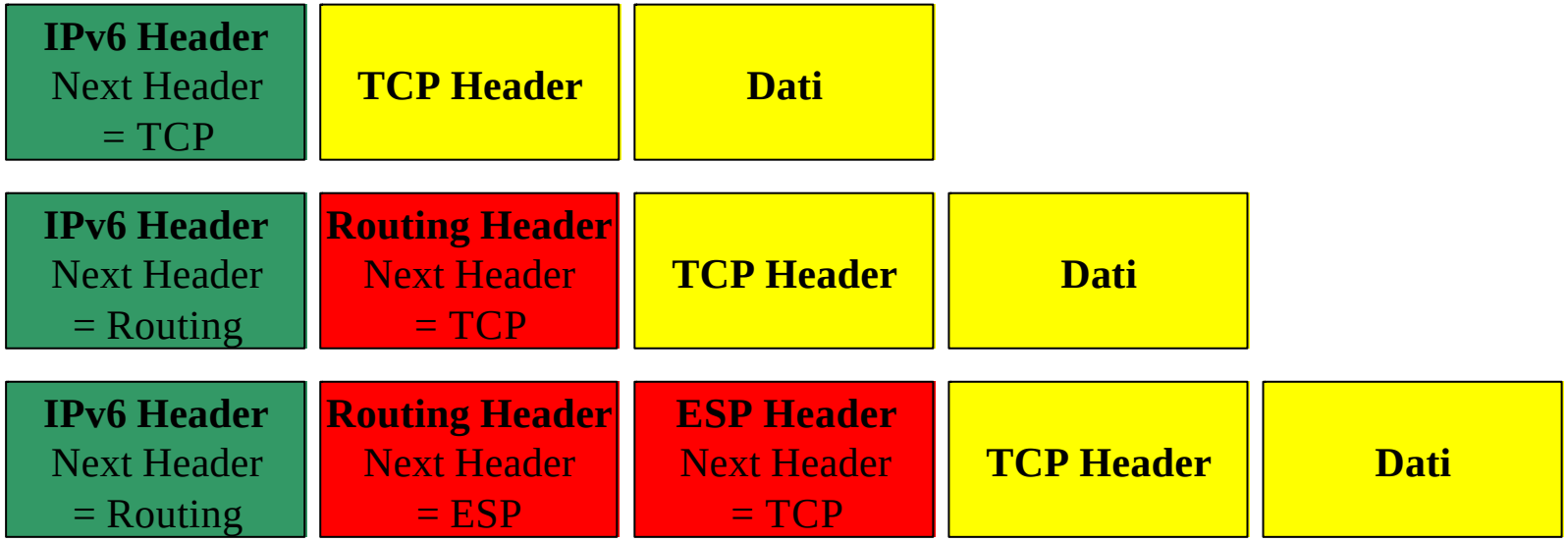
- **Flow Label**. 20 bit.
  - Utilizzo ancora non chiaro. Serve per identificare i flussi. Mobile IPv6.
  - Migliora le prestazioni rispetto ad IPv4
- **Payload Length**. 16 bit.
  - Specifica la lunghezza dei dati nel pacchetto.
  - Al max pacchetti da 64 KB. Per pacchetti di dimensioni maggiori si utilizza l'opzione Jumbo Payload

Header IPv6

- **Next Header.** 8 bit.
  - Specifica l'header successivo. Se è un protocollo di livello più alto, i valori sono compatibili con quelli specificati per IPv4.
  - Consente di specificare gli extension header.
- **Hop Limit.** 8 bit.
  - Sostituisce il TTL IPv4.
- **Source address.** 16 byte.
  - L'indirizzo IPv6 del mittente.
- **Destination address.** 16 byte.
  - L'indirizzo IPv6 del destinatario.

Extension Headers

- Un nuovo metodo per implementare le opzioni
- Aggiunto dopo l'header di base IPv6



Tipi di Headers

- **00** = Hop-by-Hop Options
- **43** = Routing
- **44** = Fragment
- **51** = Authentication
- **60** = Destination Options
- **50** = Encapsulating Security Payload
- **xx** = Protocolli di livello piu' alto come per IPv4
- **58** = Internet Control Message Protocol (ICMPv6)
- **59** = nessun next header

Tipi di Headers

- **Hop-by-hop options (00)**
  - Queste informazioni devono essere esaminate da ogni nodo lungo il percorso del pacchetto.
  - Alcune opzioni utilizzate:
    - Router Alert
    - Jumbo Payload

Tipi di Headers

- **Routing (43)**
  - Simile all'opzione IPv4 Loose Source Route
  - Indica una lista di router da attraversare.
  - Migliora le prestazioni rispetto ad IPv4
    - Header valutata solamente dai router specificati
    - Ogni router (di quelli specificati), valuta il routing header ed aggiorna la destinazione del pacchetto con l'indirizzo IPv6 del prossimo router della lista
  - Usato per il mobile IPv6 & multihoming

Tipi di Headers

- **Fragment (44)**
  - Usato soltanto dall'host mittente per l'host destinatario. (I router non frammentano più!!!)

IPv6 prevede:

- Una MTU minima di 1280 byte (68 byte in IPv4)
  - Link senza questa capacità devono gestire la frammentazione ed il riassemblaggio a livello data-link
- Che ogni nodo implementi una procedura di MTU Path Discovery (non strettamente necessario)
- Per inviare pacchetti più grandi della massima MTU consentita devo utilizzare i fragment header

Tipi di Headers

- **Destination Options (60)**
  - Usato per trasportare informazioni opzionali che saranno valutate soltanto dall'host destinatario
  - Può occupare 2 posizioni nella Daisy Chain:
    - Prima del Routing Header
    - Alla fine della Daisy Chain
  - Usato per il Mobile IPv6
    - Insieme al Routing header risolve il problema del routing "triangolare"

Tipi di Headers

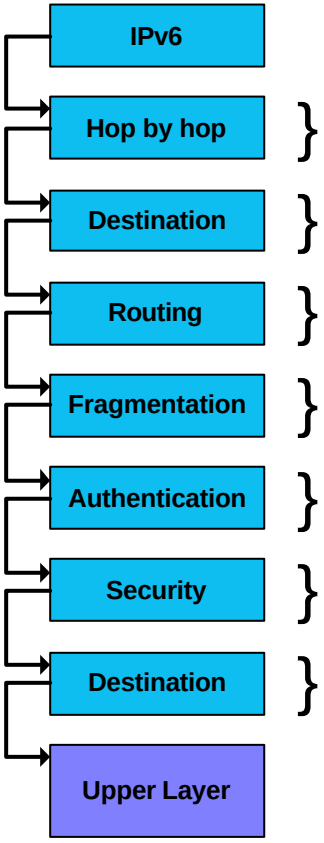
Supporto nativo alla sicurezza:

- IPsec nativo su IPv6
- Tutte le implementazioni di IPv6 dovrebbero garantire il supporto alla sicurezza. In realtà non è così!!!

- **Authentication Header (51)**
  - Fornisce l'autenticazione; un modo per verificare che l'indirizzo del mittente sia autentico e che il pacchetto non sia stato alterato durante il percorso.
- **Encapsulating Security Payload (50)**
  - Garantisce che solo il destinatario autorizzato sara' in grado di leggere il pacchetto.
  - Come in IPv4 due modalità: trasport o tunnel

Extension Headers

L’ordine nel pacchetto dovrebbe essere il seguente:



- Hop by hop: Elaborate da ogni nodo
- Destination: Elaborate da ogni Router specificato nel Routing Header
- Routing: Specificano la lista di Routers da attraversare
- Fragmentation: Elaborate dal nodo destinazione
- Authentication: Elaborate dal nodo destinazione (dopo il riassemblamento)
- Security: Cifrano il contenuto di tutto ciò che segue
- Destination: Elaborate solo dal nodo destinazione

Gli Indirizzi IPv6

Indirizzi

- IPv4 = **32 bits**
- IPv6 = **128 bits**
  - Non 4 volte il numero di indirizzi:

    4 volte il numero di bits!
  - ~3,4 * 10^{38} possibili nodi indirizzabili (max teorico)
  - 10^{30} indirizzi per ogni persona del pianeta
  - In realtà, utilizzando la stessa efficienza di assegnazione della rete IPv4 avremmo una disponibilità di ~10^{33} indirizzi IPv6

Formato dell'Indirizzo IPv6

- X:X:X:X:X:X:X:X
  - Dove X e' un campo di 16 bits in notazione esadecimale

  Es: 2001:0000:1234:0000:0000:00D0:ABCD:0532
- Il valore e' indipendente dalla notazione maiuscola o minuscola delle lettere

  Es: 2001:0000:1234:0000:0000:00D0:abcd:0532
- Gli zero a sinistra di ogni campo sono opzionali

  Es: 2001:0:1234:0:0:D0:ABCD:532

Formato dell'Indirizzo IPv6

- Campi successivi di zero sono rappresentati da **::** ma solo una volta in un indirizzo.

  Es:2001:0:1234::D0:ABCD:532

- Non e' valida la notazione:

  Es: 2001::1234::C1C0:ABCD:876

- Altri esempi:
  - **2001:760:2:0:0:0:0:0 => 2001:760:2::**
  - **FF02:0:0:0:0:0:0:1 => FF02::1**
  - **0:0:0:0:0:0:0:1 => ::1**
  - **0:0:0:0:0:0:0:0 => ::**

Indirizzi IPv6 in URL

- In una URL gli indirizzi IPv6 devono essere scritti tra parentesi quadre.

  http://[2001:1:4F3A::206:AE14]:8888/index.html

- I programmi che usano URL (browser, etc.) sono stati modificati
  - Scomodo per gli utenti
  - Prevalentemente usato per scopi diagnostici
  - Piu' comodo usare una notazione per nome a dominio.

Tipologie di Indirizzi

- IPv6 suddivide gli indirizzi in:
  - Unicast: indirizzi di nodi
  - Multicast: indirizzi di gruppi di nodi
  - Anycast: indirizzi di servizi

Architettura degli Indirizzi

Prefix	Hex	Size	Allocation
0000 0000	0000-00FF	1/256	Reserved
0000 0001	0100-01FF	1/256	Unassigned
0000 001	0200-03FF	1/128	NSAP
0000 010	0400-05FF	1/128	Unassigned
0000 011	0600-07FF	1/128	Unassigned
0000 1	0800-0FFF	1/32	Unassigned
0001	1000-1FFF	1/16	Unassigned
001	2000-3FFF	1/8	Aggregatable: IANA to registries

Da calcolare sui primi 16 bit

es. 2000-3FFF --> 0010 0000 0000 0000 – 0011 1111 1111 1111

Architettura degli Indirizzi

Prefix	Hex	Size	Allocation
010, 011, 100, 101, 110	4000-CFFF	5 * 1/8 = 5/8	Unassigned
1110	D000-EFFF	1/16	Unassigned
1111 0	F000-F7FF	1/32	Unassigned
1111 10	F800-FBFF	1/64	Unassigned
1111 110	FC00-FDFF	1/128	Unassigned
1111 1110 0	FE00-FE7F	1/512	Unassigned
1111 1110 10	FE80-FEBF	1/1024	Link-local
1111 1110 11	FEC0-FEFF	1/1024	Site-local
1111 1111	FF00-FFFF	1/256	Multicast

Indirizzi Unicast

- Unspecified
- Loopback
- IPv4 Compatible
- IPv4 Mapped
- Indirizzi Scoped:
  - Link-local
  - Site-local
- Aggregatable Global

Unspecified

- **0:0:0:0:0:0:0:0** o semplicemente **::**
- Indica l'assenza di indirizzo
- Può essere usato nella richiesta iniziale DHCP per ottenere un indirizzo
- Duplicate Address Detection (DAD)
- Come 0.0.0.0 in IPv4 (**::/0** indica la rotta di default)

Loopback

- **0:0:0:0:0:0:0:1** o semplicemente **::1**
- Identifica il nodo stesso
- Come 127.0.0.1 in IPv4 (localhost)
- Per controllare se lo stack IPv6 funziona:
  - **ping6 ::1**

IPv4 compatible

- Permettono di inserire indirizzi IPv4 in indirizzi IPv6
- I primi 96 bit sono posti a 0, gli altri 32 specificano l'indirizzo IPv4
  - 0:0:0:0:0:0:192.168.0.1
  - ::192.168.0.1
  - ::C0A8:1E01
- Utilizzati per la transizione IPv4-IPv6

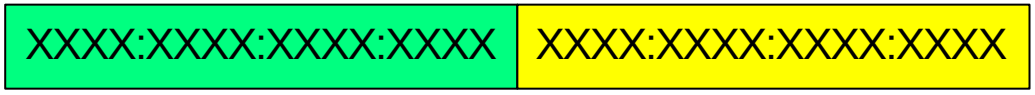
IPv4 mapped

- Permettono di definire indirizzi IPv6 per nodi che supportano solo IPv4
- I primi 80 bit sono posti a 0, i successivi 16 bit sono posti ad 1 (FFFF) e, gli ultimi 32 specificano l'indirizzo IPv4
  - 0:0:0:0:0:FFFF:192.168.0.1
  - ::FFFF:192.168.0.1
  - ::FFFF:C0A8:1E01
- Utilizzati per la transizione IPv4-IPv6

Subnet Prefix e Host Identifier

Gli indirizzi IPv6 unicast si compongono di due parti:

- Il prefisso di rete (primi 64 bit)
- L'interface ID (ultimi 64 bit)



Subnet Prefix (64 bit) **Host Identifier** (64 bit)

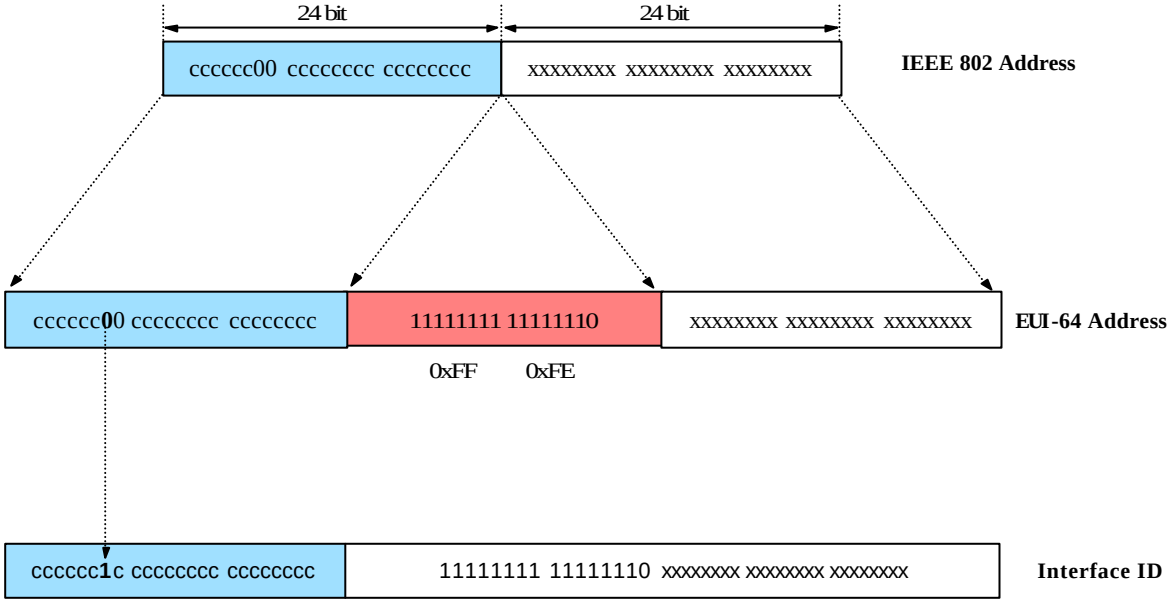
- L'host puo' essere identificato:
  - Manualmente.
  - Tramite l'identificativo di interfaccia (mac address): il mac address viene ricalcolato per essere usato come parte host dell'indirizzo IPv6 - EUI 64.

Il formato EUI-64

- L'interface ID:
  - Identifica univocamente un'interfaccia
  - Deve essere univoco su un link
  - Può essere ricavato a partire dall'identificatore EUI-64
- L'identificatore EUI-64 si basa sullo stesso principio del MAC Address di cui è l'evoluzione:
  - Identifica il produttore ed il «numero di serie» di un'apparecchiatura di qualche tipo (con 64 bit)
- Esiste una procedura che consente di passare dall'EUI-48 ID (mac-address) all'EUI-64 ID

Interface ID da mac-address

- Se si dispone, del MAC address (EUI-48 ID) si procede inserendo dopo i primi 24 bit la sequenza **FF-FE**.



MAC Address:	00-AA-00-3F-2A-1C
EUI-64 Address:	00-AA-00-FF-FE-3F-2A-1C
Complementando U/L:	02-AA-00-FF-FE-3F-2A-1C
In notazione IPV6:	02AA:00FF:FE3F:2A1C

Privacy

- Il modo precedentemente descritto ricava l'interface ID di un nodo, a partire dal suo indirizzo MAC
  - Anche se il prefisso può cambiare nel tempo, l'interface ID rimane lo stesso e quindi l'indirizzo IPv6 permette potenzialmente di tracciare un utente
  - Problema già presente con gli indirizzi statici IPv4 ma ora il problema della privacy è molto più sentito in quanto il MAC address è più associabile alla persona

- RFC 3041 specifica un modo alternativo di generare l'interface ID (stringa casuale di 64 bit)

Link e Site

- Per **link** si intende una rete fisica unica come ad esempio una LAN, un collegamento punto-punto. Nodi sullo stesso link sono detti *neighbor* (vicini)

- Un **site** è invece, un gruppo di link gestiti da un'unica autorità (ad esempio il campus di un'università)

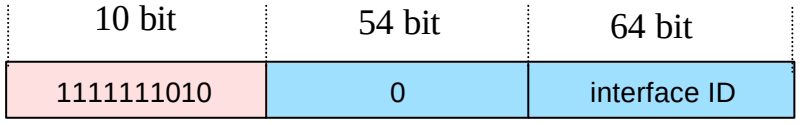
Link-local

- E’ uno Scoped address (novità di IPv6)
- Scope (ambito) = local link (*i.e. LAN*, *VLAN*)
  - Può essere usato solo fra nodi dello stesso link
  - Non puo' essere ruotato
- Fornisce ad ogni nodo un indirizzo IPv6 per iniziare le comunicazioni

Link-local

- Automaticamente configurato su ogni interfaccia
  - Usa l'interface identifier (basato sul MAC address)

- Formato:
  - **FE80:0:0:0:<*interface identifier*>**



Consortium GARR

Link-local

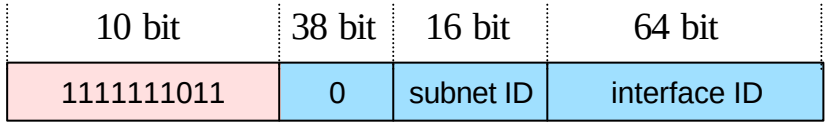
Prefix	Hex	Size	Allocation
010, 011, 100, 101, 110	4000-CFFF	5 * 1/8 = 5/8	Unassigned
1110	D000-EFFF	1/16	Unassigned
1111 0	F000-F7FF	1/32	Unassigned
1111 10	F800-FBFF	1/64	Unassigned
1111 110	FC00-FDFF	1/128	Unassigned
1111 1110 0	FE00-FE7F	1/512	Unassigned
1111 1110 10	FE80-FEBF	1/1024	Link-local
1111 1110 11	FEC0-FEFF	1/1024	Site-local
1111 1111	FF00-FFFF	1/256	Multicast

Site-local

- E’ uno Scoped address
- Scope = site (una rete di link)
  - Puo' essere usato soltanto fra nodi dello stesso site
  - Non puo' essere usato fuori dal site (es. Internet)
  - Molto simile agli indirizzi privati IPv4
- Non configurato di default

Site-local

- Formato:
  - **FEC0:0:0:<subnet id>:<interface id>**
  - Subnet id = 16 bits = 64K subnets



- Permette un piano di indirizzamento per un intero sito
- Esempi d'uso:
  - Numerare un site prima di connetterlo ad Internet.
  - Indirizzamento privato (es. stampanti locali)

Consortium GARR

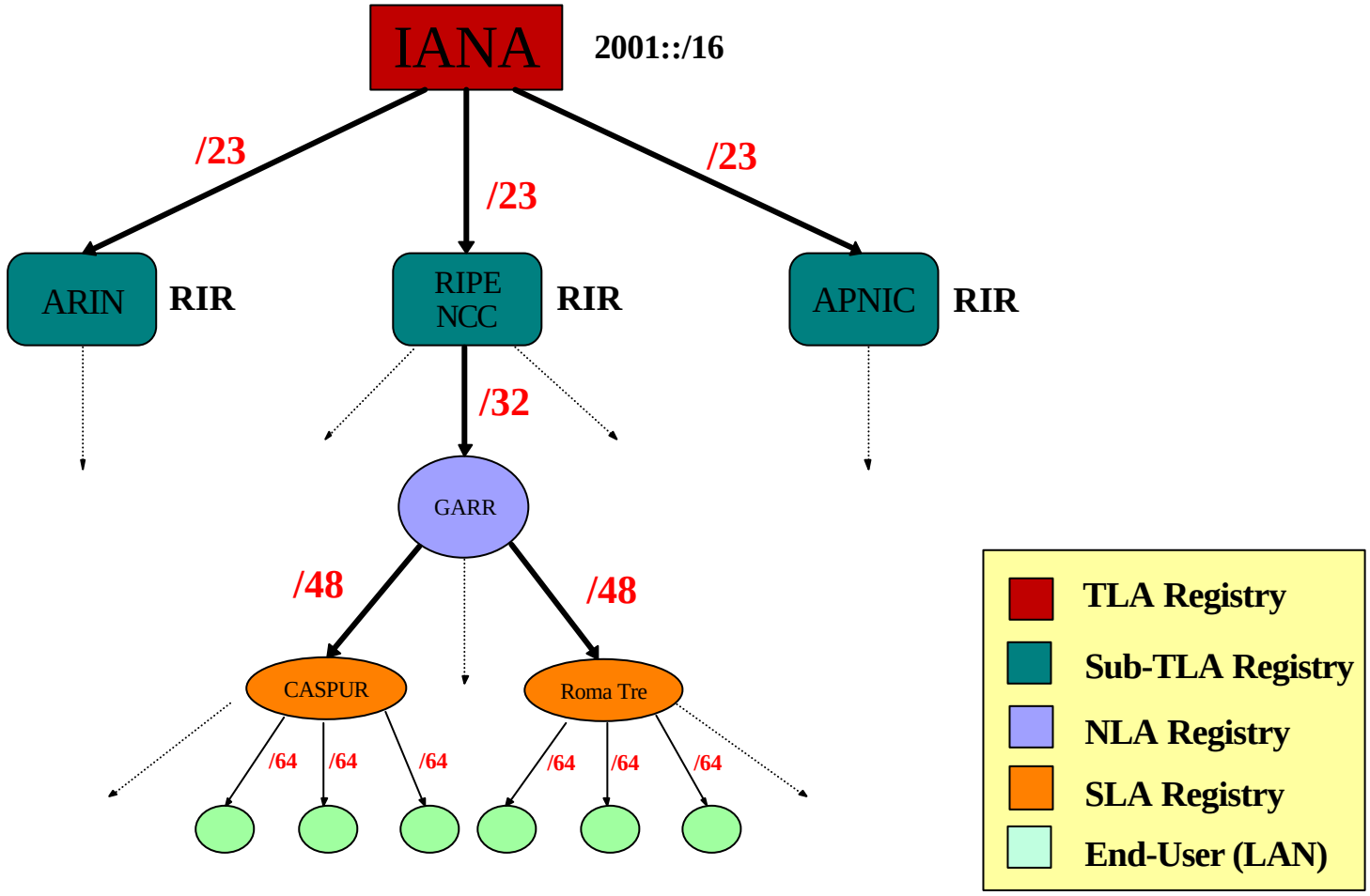
Site-local

Prefix	Hex	Size	Allocation
010, 011, 100, 101, 110	4000-CFFF	5 * 1/8 = 5/8	Unassigned
1110	D000-EFFF	1/16	Unassigned
1111 0	F000-F7FF	1/32	Unassigned
1111 10	F800-FBFF	1/64	Unassigned
1111 110	FC00-FDFF	1/128	Unassigned
1111 1110 0	FE00-FE7F	1/512	Unassigned
1111 1110 10	FE80-FEBF	1/1024	Link-local
1111 1110 11	FEC0-FEFF	1/1024	Site-local
1111 1111	FF00-FFFF	1/256	Multicast

Aggregatable Global

- La politica di assegnazione degli indirizzi IPv6 è ancora in discussione. Al momento è usata una policy provvisoria:
  - /23 Regional Registries
  - /32 Local Internet Registries
  - /48 Site
    - 2^{16} subnets per site = 65536 subnets
  - /64 Link

Allocazione degli indirizzi IPv6



La situazione attuale

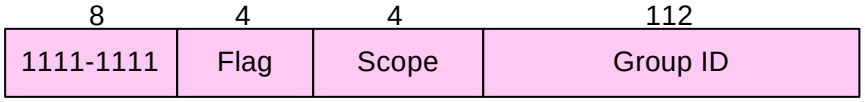
- RIPE NCC ha ottenuto da IANA 4 /23:
  - 2001:0600::/23
  - 2001:0800::/23
  - 2001:0A00::/23
  - 2001:1400::/23
- GARR ha ricevuto da RIPE NCC il blocco di indirizzi:
  - 2001:0760::/32

Multicast

- Multicast = uno a tanti
- Non esiste il **broadcast** in IPv6. Multicast e' usato al suo posto, soprattutto nei link locali
- Scoped addresses: sostituisce il TTL di IPv4

Multicast

- Formato:
  - **FF<flags><scope>::<group id>**
  - Identificati da FP **11111111** (=**FF**)
  - Flag = 0 permanente / 1 temporaneo
  - Scope: **node** (1), **link** (2), **site** (5), **organization** (8), **global** (E)
  - Group ID: identifica un gruppo multicast in un dato scope



Multicast

- Ad esempio, considerando il *Group ID* **All-Nodes (1)** avremo che:
  - All'indirizzo **FF01::1** partecipano tutte le interfacce sullo stesso *nodo*
  - All'indirizzo **FF02::1** partecipano tutte le interfacce sullo stesso *link*
  - All'indirizzo **FF05::1** partecipano tutte le interfacce sullo stesso *site*
  - All'indirizzo **FF0E::1** partecipano tutte le interfacce su *internet*

Indirizzi Multicast

- Alcuni indirizzi multicast riservati:

INDIRIZZO	SCOPE	TIPO
FF01::1	Node	All Nodes
FF02::1	Link	All Nodes
FF01::2	Node	All Routers
FF02::2	Link	All Routers
FF05::2	Site	All Routers
FF02::1:FFXX:XXXX	Link	Solicited-Node

Anycast

- Gli indirizzi Anycast non sono distinguibili dagli indirizzi unicast
  - Sono indirizzi unicast assegnati ad un insieme di interfacce (normalmente di nodi diversi)
  - Ai nodi deve essere esplicitamente detto che gli si sta assegnando un indirizzo anycast
- Indicano il server più vicino ad un mittente
- Alcuni indirizzi anycast sono riservati per usi specifici:
  - Router subnet
  - Mobile IPv6 home-agent discovery

Indirizzi per ogni host

- Ogni host IPv6 deve riconoscere come propri i seguenti indirizzi:
  - Un indirizzo *link-local* per ogni interfaccia
  - Gli indirizzi *unicast/anycast* assegnati (manualmente o automaticamente)
  - L'indirizzo di *Loopback*
  - L'indirizzo del gruppo *All-Nodes multicast*
  - Gli indirizzi *Solicited-node multicast* per ogni indirizzo *unicast/anycast* assegnato
  - Gli indirizzi *multicast* di tutti gli altri gruppi di cui l'host fa parte

Selezionare un indirizzo

- Un nodo può utilizzare vari prefissi di rete
  - Quindi può avere più indirizzi IPv6 assegnati alla stessa interfaccia (può utilizzare, ad esempio, anche diversi indirizzi IPv6 globali)
- Quale sarà usato come sorgente e destinazione per ogni flusso?
- La scelta viene fatta principalmente in base a queste regole:
  - Usare il giusto scope in base alla destinazione (global, site, local)
  - Usare l'indirizzo più simile alla destinazione (IPv4, IPv6)
- L'algoritmo di scelta può essere sovrascritto dallo stack oppure dall'applicazione

Riferimenti

RFC2373

IP Version 6 Addressing Architecture

RFC2374

An IPv6 Aggregatable Global Unicast Address Format

RFC3041

Privacy Extensions for Stateless Address Autoconfiguration

IETF internet-draft

Default Address Selection for IPv6

Riferimenti

RFC 2711

IPv6 Router Alert Option

RFC 2675

IPv6 Jumbograms

Consortium GARR

ICMPv6
Neighbor Discovery
Configurazione degli indirizzi

Consortium GARR

ICMPv6

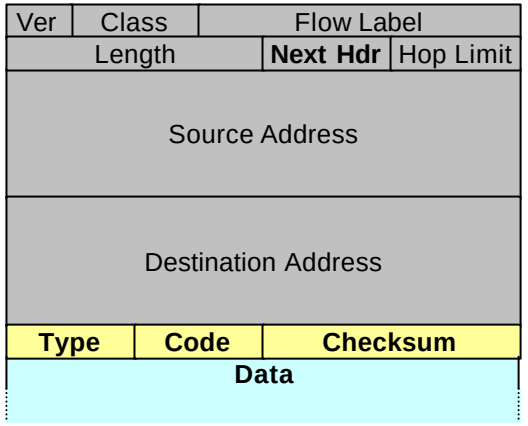
Protocollo e tipi di pacchetto

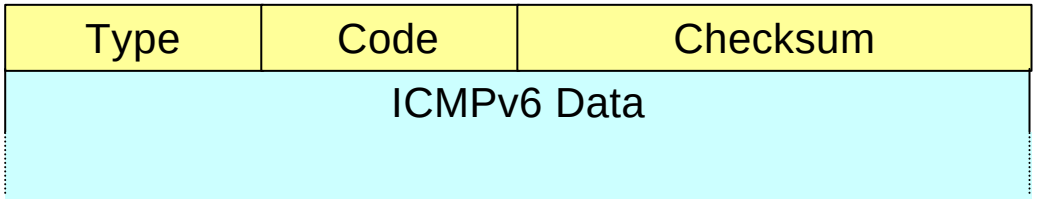
Il protocollo ICMPv6

- Equivalente IPv6 di ICMP
- Stesse funzionalità di base
  - Segnalazione errori, controllo, diagnostica
- Aggiunge nuove funzionalità
  - Neighbor discovery
    - Neighbor Solicitation, Unreachability, Autoconfigurazione
  - Gestione dei gruppi multicast
- Accorpa in un unico protocollo le funzioni svolte in IPv4 da ICMP, ARP, e IGMP

ICMPv6: Formato dei pacchetti

- IPv6 Next Header = 58
  - Diverso da ICMP in IPv4
- Nell'header ICMPv6:
  - ICMPv6 Type (Tipo)
  - ICMPv6 Code (Specifica ulteriore)
  - Header Checksum (intestazioni ICMPv6 e IPv6)
  - ICMPv6 Data





ICMPv6: Tipi di messaggi

- Il primo bit del campo Type distingue tra due classi di messaggi:
  - I tipi da 0 a 127 sono segnalazioni di errore (Error Messages)
  - I tipi da 128 a 255 sono messaggi informativi (Informational Messages)
- I messaggi di errore sono:
  - Destination Unreachable (1)
  - Packet Too Big (2)
  - Time Exceeded (3)
  - Parameter Problem (4)

ICMPv6: Messaggi informativi

- Diagnostica
  - Echo request/Echo reply (128/129)
- Controllo
  - Gestione dei gruppi multicast
    - Multicast Listener Query/Report/Done (130/131/132)
  - Neighbor discovery
    - Router Solicitation/Advertisement (133/134)
    - Neighbor Solicitation/Advertisement (135/136)
    - Redirect (137)
    - Inverse Neighbor Discovery (141/142)
- Richiesta di informazioni
  - Node Information Query/Response (139/140)

Tabella dei tipi di messaggio

1	Destination Unreachable	133	Router Solicitation
2	Packet Too Big	134	Router Advertisement
3	Time Exceeded	135	Neighbor Solicitation
4	Parameter Problem	136	Neighbor Advertisement
		137	Redirect Message
128	Echo Request	138	Router Renumbering
129	Echo Reply	139	ICMP Node Information Query
130	Multicast Listener Query	140	ICMP Node Information Response
131	Multicast Listener Report	141	Inverse Neighbor Disc. Solicitation
132	Multicast Listener Done	142	Inverse Neighbor Disc. Advertisement

Consortium GARR

ICMPv6

Path MTU discovery

Path MTU Discovery (1)

- In IPv6 la frammentazione è end-to-end
  - I router non frammentano i pacchetti
  - Se ne occupa l'host sorgente
- L'host deve sapere l'MTU del collegamento
- Usa la procedura di Path MTU Discovery
  - Basata su messaggi ICMPv6 "Packet too big"
    - Generati dai router quando la linea su cui va inoltrato un pacchetto ha MTU inferiore alle dimensioni del pacchetto
    - Riportano, nel campo dati, l'MTU da utilizzare

Path MTU Discovery (2)

- Procedimento:
  - Il nodo manda il primo pacchetto con una dimensione pari all'MTU del proprio link
  - Se riceve un messaggio d'errore "Packet Too Big", manda un nuovo pacchetto con le dimensioni indicate nel messaggio
  - Ripete finché non riceve più errori
- Periodicamente il nodo manda pacchetti di dimensioni maggiori per rinnovare la stima
- L'MTU minima in IPv6 è 1280 byte

Consortium GARR

Neighbor Discovery

Funzionalità di base

Neighbor Discovery

- Usa pacchetti ICMPv6
- Gestisce le informazioni di controllo all'interno di un link
  - Address resolution
    - Neighbor Solicitation e Neighbor Advertisement
    - Neighbor Unreachability Detection
  - Autoconfigurazione
    - Router Solicitation e Router Advertisement
  - Redirect
- I messaggi non possono uscire dal link
  - Sono validi solo se hanno Hop Limit = 255

Redirect

- Simile all'ICMP redirect in IPv4
- Un router informa un host che esiste un router migliore sul link per raggiungere la destinazione, oppure che la destinazione e' sul link
  - A differenza di IPv4, il redirect implica che il next hop (o la destinazione) sia sullo stesso link
    - Il link potrebbe avere dei prefissi che il nodo non conosce (es. in caso di reti NBMA o shared media)
  - Il messaggio di redirect include l'indirizzo link local e l'indirizzo di livello 2 del next hop o della destinazione
- La verifica che l'Hop Limit sia pari a 255 riduce i problemi di sicurezza presenti in IPv4

Neighbor Solicitation (1)

- Equivalente IPv6 di ARP
- Usa pacchetti ICMPv6 anziché ARP
  - Indipendente dal mezzo trasmissivo
  - Può utilizzare i meccanismi di autenticazione e cifratura previsti da IPSEC
- Usa indirizzi multicast anziché broadcast
    - Maggiore efficienza
      - Multicast di livello 2
      - I nodi non interessati possono scartare il pacchetto già allo strato IP senza esaminarne il contenuto

Neighbor Solicitation (2)

- Per ottenere un indirizzo fisico di un altro nodo:
  - Il nodo calcola l'indirizzo (multicast) Solicited-Node corrispondente all'indirizzo IPv6 del destinatario
  - Il nodo invia a questo indirizzo un pacchetto di Neighbor Solicitation specificando l'indirizzo IPv6 del destinatario nel campo dati
- Il destinatario, se presente, risponde con un pacchetto di Neighbor Advertisement
  - Il suo indirizzo fisico è specificato nella porzione dati del pacchetto
  - Viene memorizzato nella Neighbor Cache (equivalente IPv6 della ARP cache)

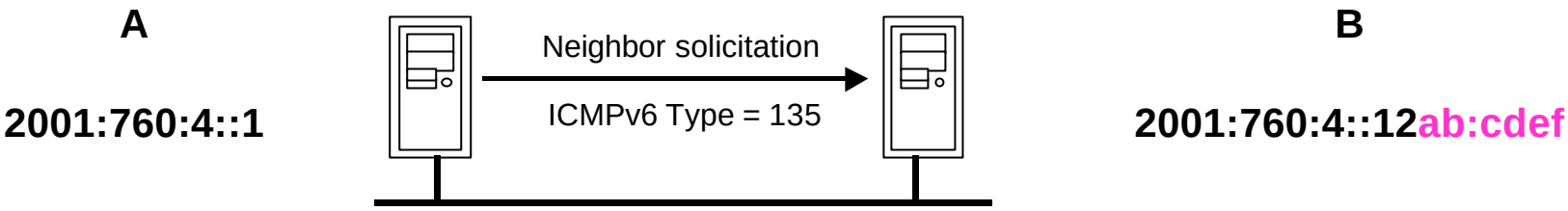
Indirizzi Solicited-Node Multicast

- Ad ogni indirizzo IPv6 unicast corrisponde un indirizzo multicast Solicited-Node

- Formato aggiungendo gli ultimi 24 bit dell'indirizzo al prefisso **ff02::1:ff00:0/104**
  - Riduce le collisioni in caso di indirizzi formati da Interface ID hardware
  - Riduce il numero di gruppi multicast a cui partecipare in caso di indirizzi multipli con lo stesso Interface ID

Indirizzo MAC
00:04:76:22:5b:a0
→
Interface ID
204:76ff:fe22:5ba0
→
Indirizzo Solicited-Node
ff02::1:ff22:5ba0

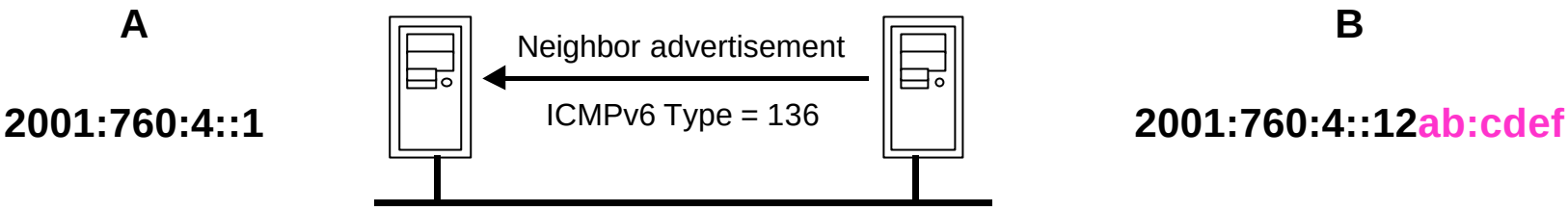
Neighbor Solicitation: esempio



- A vuole ottenere l'indirizzo fisico di B
- Calcola l'indirizzo multicast Solicited-Node corrispondente all'indirizzo IPv6 di B:

  ff02::1:ffab:cdef
- Invia un pacchetto di Neighbor Solicitation:
  - Sorgente: indirizzo IPv6 di A
  - Destinatario: indirizzo solicited-node calcolato
  - Dati ICMPv6:
    - Indirizzo IPv6 di B
    - Indirizzo fisico di A (indica a B l'indirizzo a cui rispondere)

Neighbor Solicitation: esempio



- B risponde con un pacchetto di Neighbor Advertisement:
  - Sorgente: indirizzo IPv6 di B
  - Destinatario: indirizzo IPv6 di A
  - Dati ICMP:
    - Indirizzo IPv6 di B
    - Indirizzo fisico di B

Neighbor Unreachability Detection

- Algoritmo che permette di individuare rapidamente guasti o cambiamenti di indirizzo fisico
  - Più efficiente di un semplice timeout
  - Utile per nodi mobili che si spostano da un link all'altro
- Ogni nodo tiene traccia dello stato di raggiungibilità dei nodi vicini
  - Utilizzando informazioni provenienti dai protocolli di strato superiore (es. ACK di TCP)
    - Nodi vicini: funzionamento del nodo
    - Nodi remoti: funzionamento del router next-hop
  - Inviando al nodo pacchetti di Neighbor Solicitation

NUD: Funzionamento

- Se un nodo non ha informazioni sulla raggiungibilità di un vicino, gli invia pacchetti unicast di Neighbor Solicitation in parallelo al traffico normale
- Se non ottiene risposta, cancella il vicino dalla Neighbor Cache e ripete il procedimento di Neighbor Solicitation
  - Il nodo potrebbe aver cambiato indirizzo fisico
- Se questo fallisce, il vicino è irraggiungibile
  - Le conseguenze dipendono dal tipo di vicino:
    - Host: viene notificato un errore ai protocolli di strato superiore
    - Router: il nodo seleziona un altro router

Autoconfigurazione stateless

- Permette ai nodi IPv6 di connettersi alla rete senza dover configurare manualmente gli indirizzi
  - Non è necessario utilizzare un server DHCP
  - Il link deve supportare il multicast
- Gli indirizzi sono basati sugli Interface ID
  - Possibile perché gli Interface ID sono univoci a livello mondiale
- I nodi possono comunicare tra loro utilizzando gli indirizzi link-local
  - Gli indirizzi link-local sono ottenuti autonomamente
  - Una rete peer-to-peer non richiede configurazione
- Il server DNS deve essere specificato a mano

Configurazione stateful

- Gli indirizzi e gli altri parametri di rete (es. DNS) possono essere configurati anche manualmente:
  - Configurazione interamente manuale
  - DHCPv6 (standard ancora in via di definizione)
  - Autoconfigurazione stateless
    - I Router Advertisement contengono due flag che specificano le modalità di configurazione:
      - “Managed Address Configuration”: indica se l’host deve ottenere anche indirizzi da DHCPv6
      - “Other Stateful Configuration”: indica se l’host deve utilizzare DHCPv6 per ottenere altre informazioni di configurazione (es. server DNS, server NTP, ...). Sempre vero se Managed Address Configuration è vero.

DHCPv6

- Viene utilizzato solo se sul link non sono presenti router oppure se i Router Advertisement ne specificano l'utilizzo
- Gli indirizzi ottenuti si aggiungono a quelli eventualmente ottenuti tramite autoconfigurazione
- Funzionamento:
  - Simile a DHCP per IPv4
  - Il server mantiene informazioni sullo stato dei client
  - Permette di configurare gli indirizzi IPv6 e/o fornire altre informazioni come server DNS o NTP
  - Utilizza il protocollo UDP
  - Utilizza gli indirizzi multicast ff02::1:2 (all DHCP agents, link-local scope) e ff05::1:3 (all DHCP servers, site-local scope)