



Marco Listanti

IPv6



Marco Listanti

IPv6: funzionalità e formato del pacchetto



Funzionalità IPv6 (1)

- **Aumento dello spazio di indirizzamento**
 - Indirizzi a 128 bit
 - Indirizzamento gerarchico basato sul concetto di prefisso
- **Semplificazione della struttura dell'header dei pacchetti**
 - Header di lunghezza fissa
 - Diversa modalità di codifica del campo "Options"
 - Eliminazione dei campi checksum e quelli dedicati alla frammentazione
- **Possibilità di identificazione dei flussi dei pacchetti**
 - Flow label
- **Meccanismo integrato di autoconfigurazione delle interfacce di rete**
- **Integrazione con l'architettura IPSec**

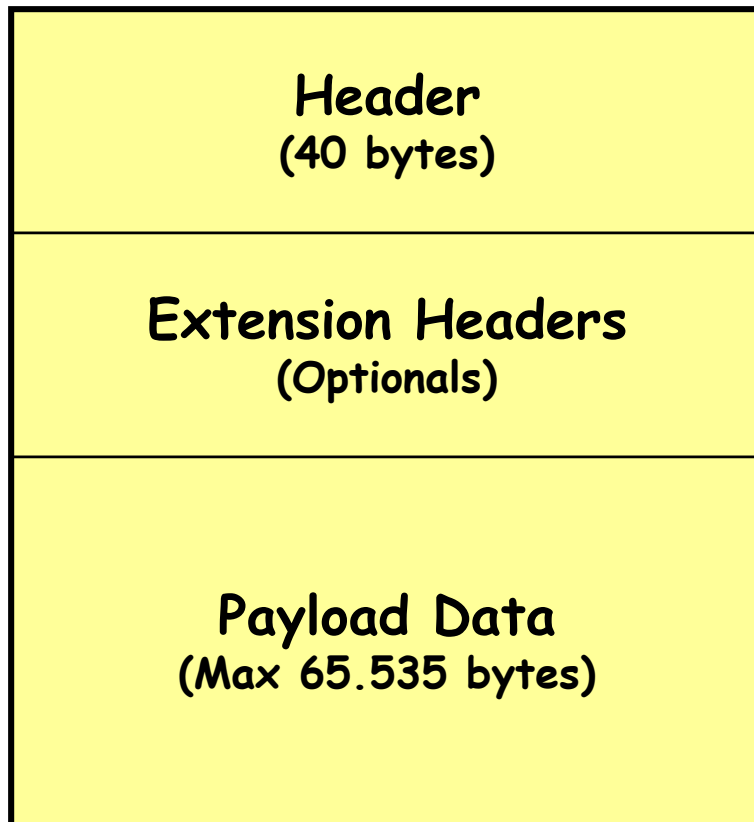


Funzionalità IPv6 (2)

- **Le funzioni e il formato dei pacchetti IPv6 sono specificate nei seguenti RFC**
 - RFC 2460: Internet Protocol, Version 6 (IPv6) Specification
 - RFC 3513: IP version 6 Addressing Architecture
 - RFC 3587: IPv6 Global Unicast Address Format
 - RFC 3177: IAB/IESG Recommendations on IPv6 Address Allocations to Sites
 - RFC 2461: Neighbor Discovery for IP version 6 (IPv6)
 - RFC 2462: IPv6 stateless address autoconfiguration
 - RFC 2893: Transition mechanism for IPv6 hosts and routers
 - RFC 3056: Connection of IPv6 domains via IPv4 clouds
 - RFC 3315: Dynamic Host Configuration Protocol for IPv6 (DHCPv6)



Formato del pacchetto IPv6



- **Header**
 - contiene le informazioni comuni a tutti i pacchetti
- **Extension Headers**
 - contengono le opzioni utilizzate dai router intermedi e/o dall'host di destinazione
- **Payload Data**
 - sono i bit informativi elaborati dall'host di destinazione



IPv6 Datagram Basic Header

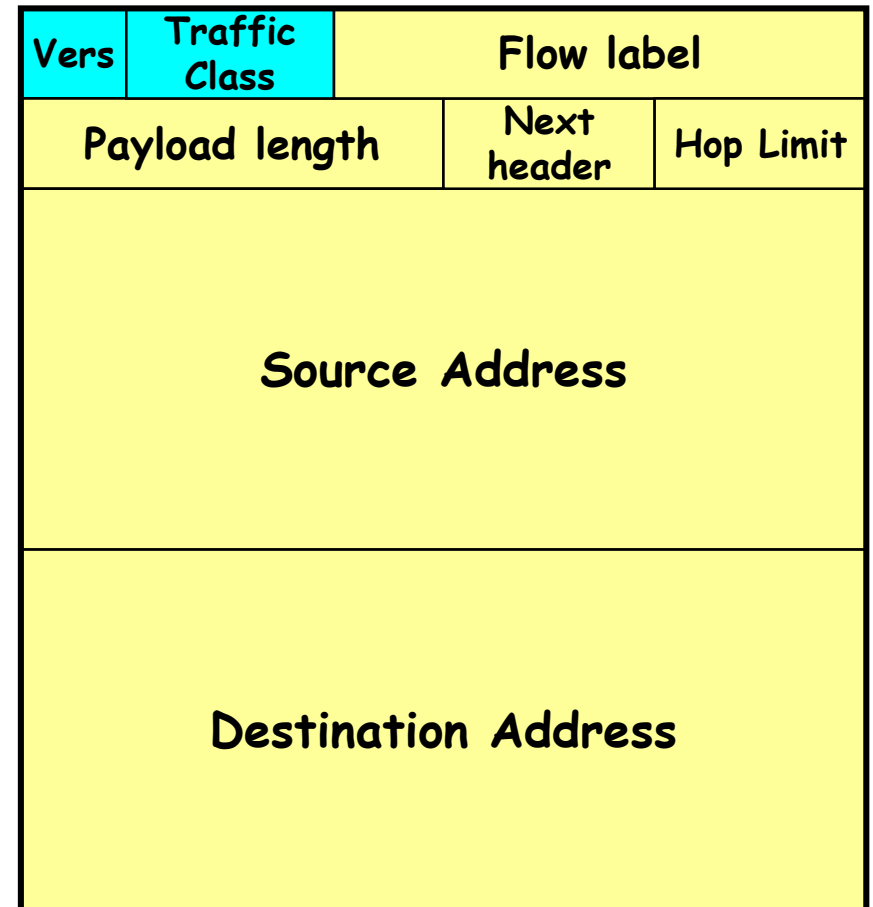
■ Version (4 bit)

- versione del protocollo, è possibile la coesistenza di più versioni di IP

■ Traffic Class (8 bit)

- Stabilisce la classe di servizio e la priorità del pacchetto
- E' compatibile con la specifica del campo DSCP dell'architettura Diffserv

0 4 8 12 16 20 24 28 31





IPv6 Datagram Basic Header

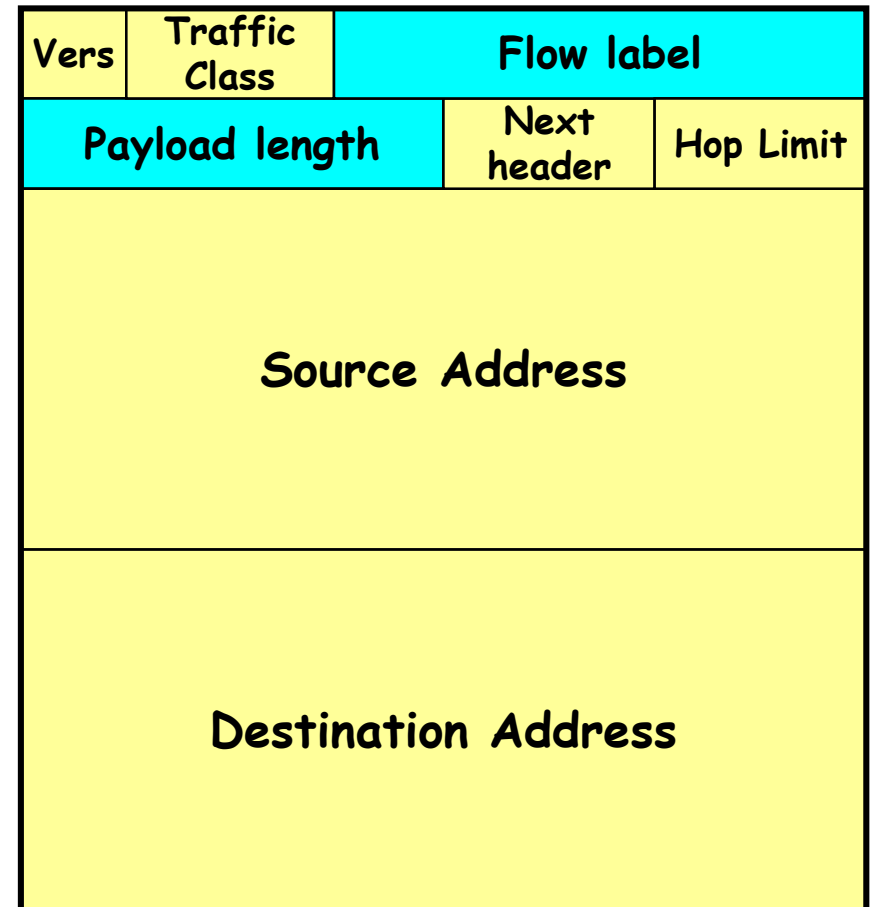
■ Flow label (20 bit)

- Identifica, insieme al campo source address, un particolare flusso di pacchetti
- Consente di instradare i pacchetti in hardware
- Consente l'applicazione delle procedure di riservazione di risorse per traffico con qualità di servizio garantita

■ Payload Length (16 bit)

- Lunghezza in byte del pacchetto IP (escluso l'header)
- Normalmente la lunghezza massima del payload è 65.535 byte
- Se la lunghezza del pacchetto è maggiore di 64 K il suo valore è "0", l'opzione "jumbo payload" indica la lunghezza effettiva

0 4 8 12 16 20 24 28 31





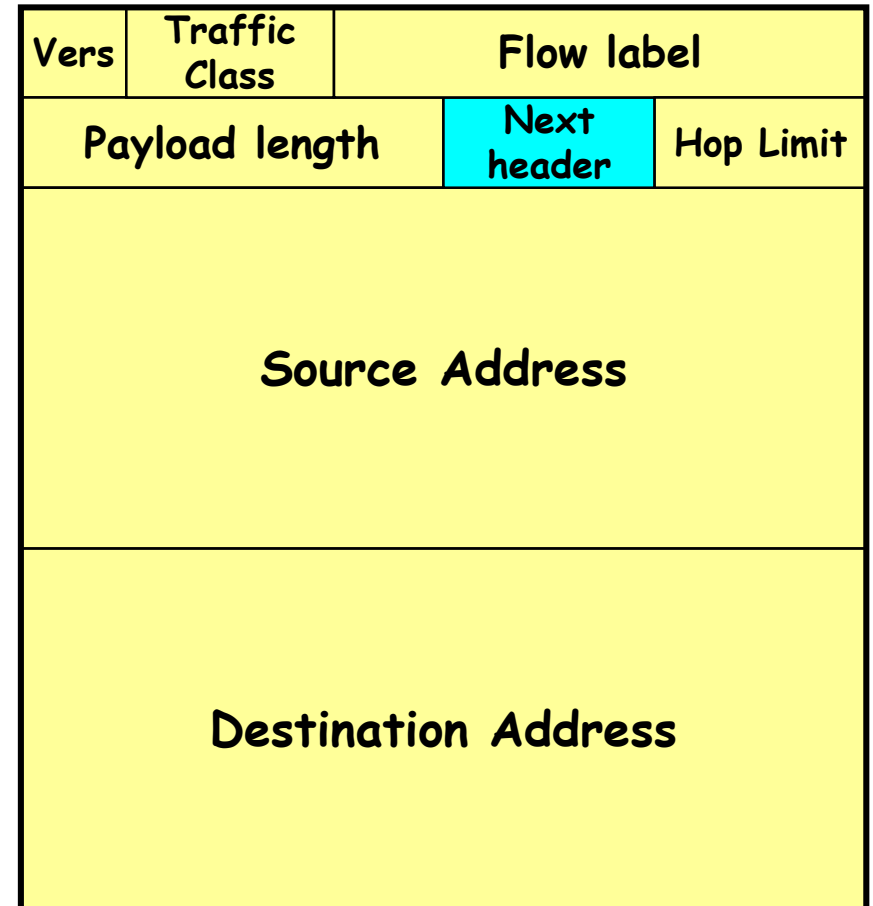
IPv6 Datagram Basic Header

■ Next Header (8 bit)

- Contiene il codice che identifica l'header che segue nel pacchetto

0	Hop-by-hop options header
4	Internet Protocol (IP)
6	Transmission Control Protocol (TCP)
17	User Datagram Protocol (UDP)
43	Routing
44	Fragment Header
50	Encapsulating Security Payload
51	Authentication Header
58	Internet Control Message Protocol
59	No Next Header
60	Destination Options Header

0 4 8 12 16 20 24 28 31





IPv6 Datagram Basic Header

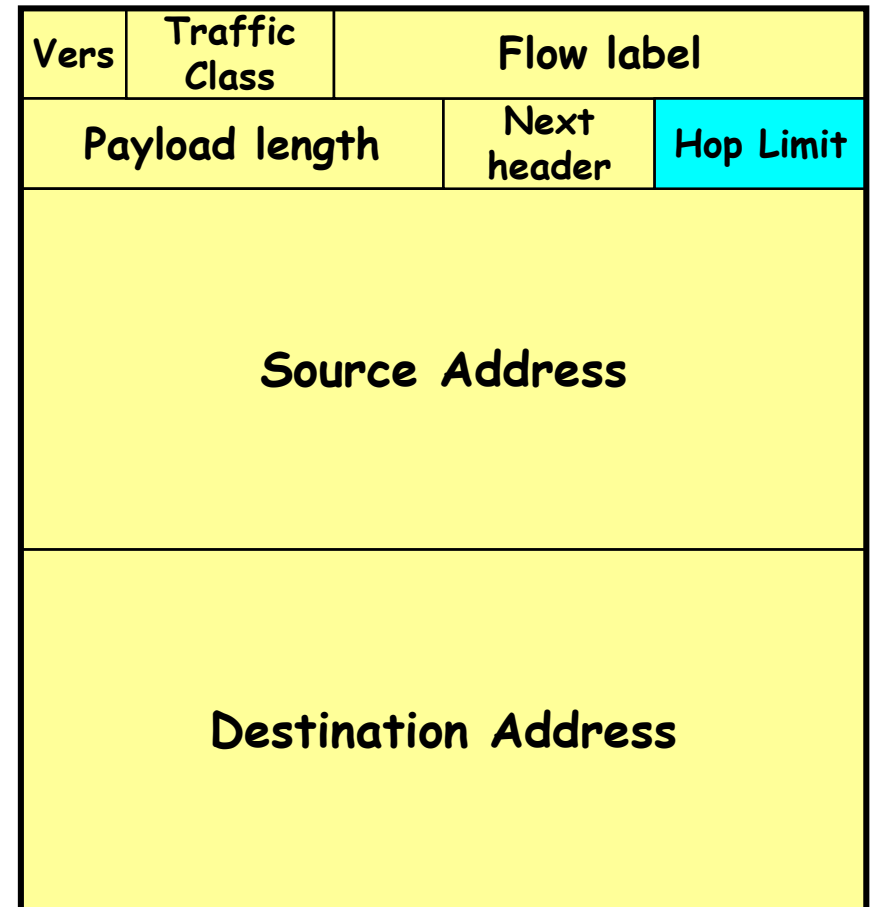
■ Hop Limit (8 bit)

- numero massimo di tratte di rete che il pacchetto può attraversare
- ogni router decrementa di una unità tale campo
- se il contatore si azzera prima che la destinazione sia raggiunta, il datagramma è scartato
- evita gli effetti di eventuali loop in rete e può essere utilizzato per effettuare delle ricerche di host in rete a distanza prefissata

■ Source e Destination Address (128 bit)

- indicano gli indirizzi IP degli host sorgente e di destinazione

0 4 8 12 16 20 24 28 31





IPv6 Extension Headers (1)

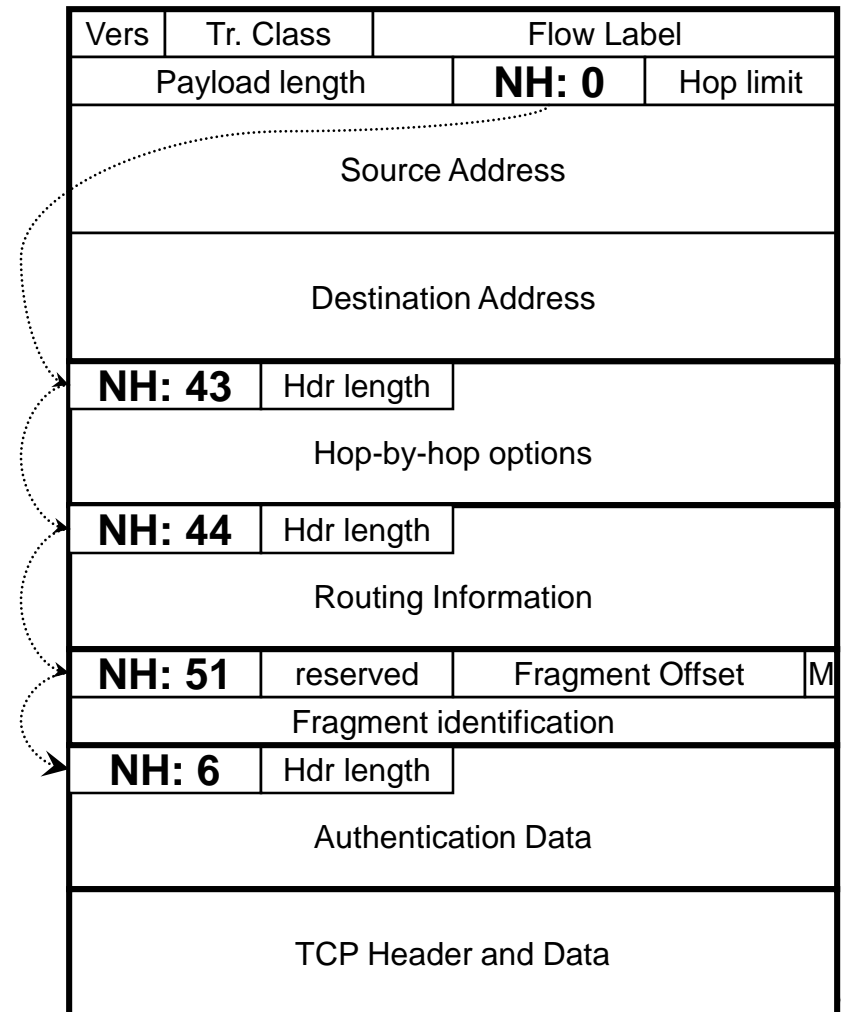
- Sono utilizzati per inviare informazioni opzionali alla destinazione o ai sistemi intermedi
- Sono definiti 6 tipi di Extension Headers (EH)

Next Header	Extension Header
0	Hop-by-hop options header
43	Routing Header
44	Fragment Header
51	Authentication Header
50	Encapsulation Security Payload Header
60	Destination Options Header



IPv6 Extension Headers (2)

- Un pacchetto può trasportare un numero qualsiasi di EH
- Ciascun EH è identificato dal valore del campo *Next Header* dell'header che lo precede
- Tutti gli EH tranne l'Hop-by-Hop sono elaborati dal nodo identificato dal destination address
- Il formato generale di un EH prevede:
 - Next Header (8 bit): identifica l'EH successivo
 - Hdr Length (8 bit): lunghezza dell'EH esclusi i primi 8 ottetti





IPv6 Extension Headers (3)

- L'ordine di inserimento degli EH nel pacchetto è il seguente
 - IPv6 header
 - Hop-by-hop options header
 - Destination options header
 - opzioni che devono essere elaborate dal nodo che appare nel campo Destination Address e, successivamente, dalle seguenti destinazioni indicate nel Routing header
 - Routing header
 - Fragment header
 - Authentication header
 - Encapsulating Security Payload header
 - Destination Options header
 - Opzioni che devono essere elaborate dal nodo destinazione finale
 - Upper-layer header



Hop-by-Hop Options Header (1)

- Contiene informazioni che devono essere elaborate da ogni sistema intermedio sul percorso del pacchetto
- È identificato dal codice Next Header = 0
- E' costituito dai seguenti campi
 - Type (8 bit): indica il tipo di opzione
 - Length (8 bit): indica la lunghezza del campo Data
 - Data (multiplo di 64 bit): trasporta il valore dell'opzione e alcune indicazioni per il router utili per l'elaborazione dell'opzione

Next Header	Header length	Type	Length
Data			



Hop-by-Hop Options Header (2)

- I primi due bit del campo Type indicano la reazione che un router deve avere nel caso non riconosca l'opzione

Type	Action
00xxxxxx	Ignora l'opzione e elabora ugualmente il datagramma
01xxxxxx	Scarta il datagramma
10xxxxxx	Scarta il datagramma ed invia un messaggio ICMP
11xxxxxx	Scarta il datagramma ed invia un messaggio ICMP solo se la destinazione non è multicast

- Il terzo bit stabilisce se il campo "data" può essere modificato

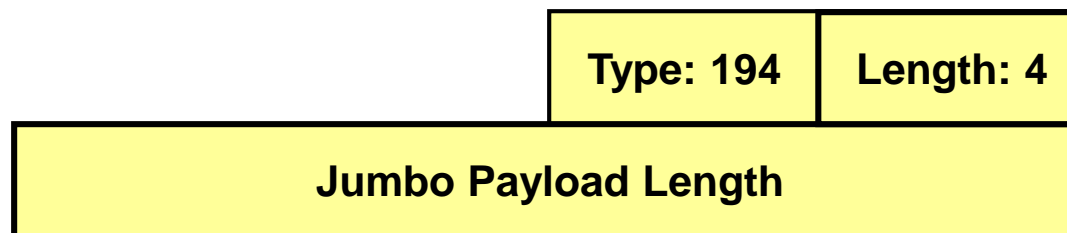
Type	Action
xx0xxxxx	Il campo "data" non deve essere modificato
xx1xxxxx	Il campo "data" può essere modificato



Hop-by-Hop Options Header (3)

■ Jumbo Payload Length Option

- È individuata dal valore 194 del campo Type
- serve ad aumentare la lunghezza massima del pacchetto rispetto a quanto consentito dall'header principale
- nel caso tale opzione sia utilizzata il campo payload length del basic header deve contenere il valore 0
- Il campo data ha lunghezza 32 bit
- La lunghezza massima del pacchetto è quindi $2^{32}-1$ byte





Routing Header (1)

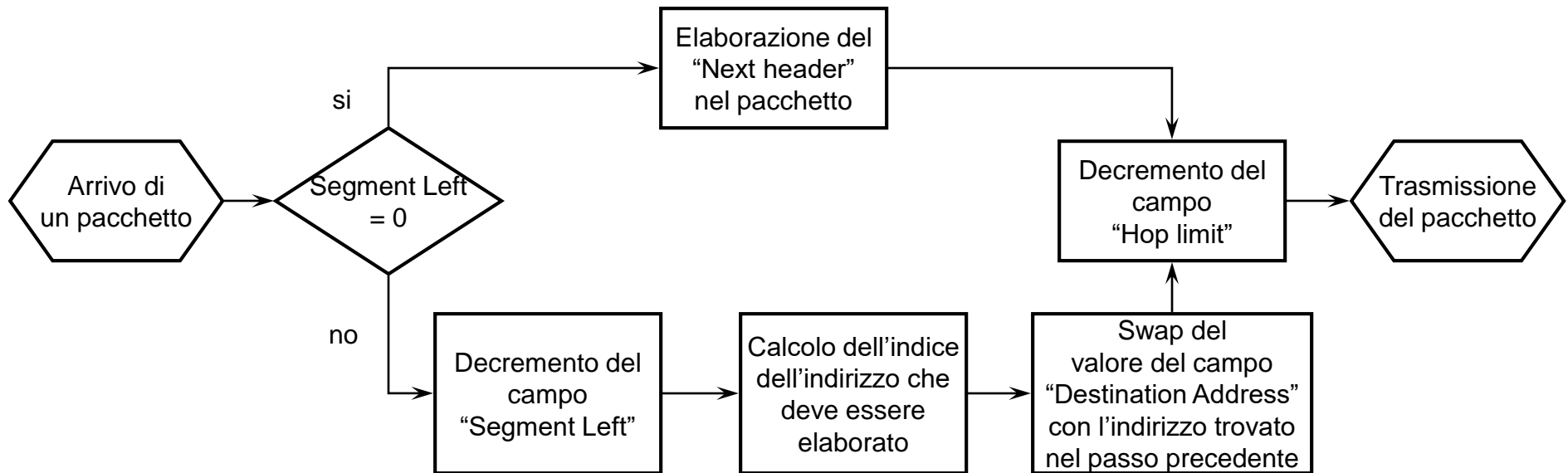
Next Header	Hdr Length	Type: 0	Segment Left
Reserved			
Address [0]			
Address [1]			
.			
Address [n-1]			

- Permette l'instradamento di un pacchetto su un cammino predefinito
- Fornisce ai router indicazioni per l'instradamento del datagramma
- Segment left (8 bit)
 - indica il numero di indirizzi che devono essere ancora elaborati
 - ogni router decrementa tale campo
 - Se il campo ha valore "0" il router ignora l'intero "extension header"



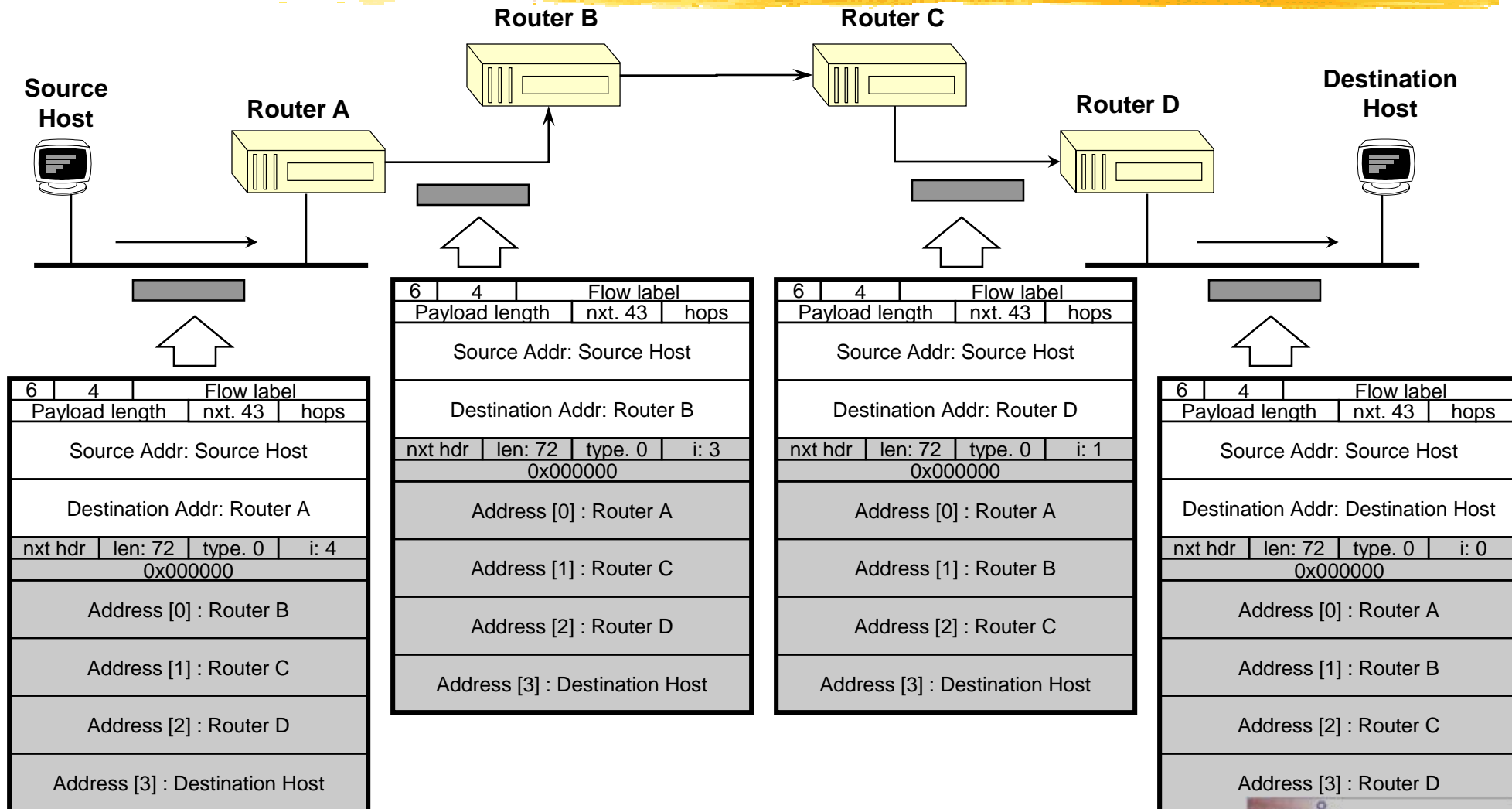
Routing Header (2)

- L'algoritmo che viene eseguito da un nodo che riceve un pacchetto che contiene un Routing Header





Routing Headers (3)





Marco Listanti

IPv6: Indirizzamento



Indirizzamento IPv6 (1)

- **Dimensione 128 bit (16 bytes)**
 - Lo spazio equivale a circa $340 \cdot 10^{36}$ indirizzi
 - Utilizzato con la stessa efficienza dello spazio degli indirizzi IPv4 consente di gestire circa 50.000 indirizzi per metro quadro
- **Un indirizzo è rappresentato da otto numeri esadecimali (ogni numero equivale a 16 bit) divisi dal simbolo ":"**
 - FE80:0000:0000:0000:0001:0800:23E7:F5DB
- **Si possono omettere i gruppi di "0" iniziali in ogni numero**
 - FE80:0:0:0:1:800:23E7:F5DB
- **Si possono omettere completamente un gruppo (uno solo) di numeri consecutivi di valore "0" sostituendoli con il simbolo "::"**
 - FE80::1:800:23E7:F5DB



Indirizzamento IPv6 (2)

- **Sono definiti tre tipi di indirizzi**
 - **Unicast**
 - Identifica una singola interfaccia
 - Un pacchetto che reca un indirizzo di questo tipo è consegnato esclusivamente a quella interfaccia
 - **Anycast**
 - Identifica un insieme di interfacce
 - Un pacchetto che reca un indirizzo di questo tipo è consegnato ad una delle interfacce identificate dall'indirizzo (normalmente la più vicina)
 - **Multicast**
 - Identifica un insieme di interfacce
 - Un pacchetto che reca un indirizzo di questo tipo è consegnato a tutte le interfacce identificate dall'indirizzo



Indirizzamento IPv6 (3)

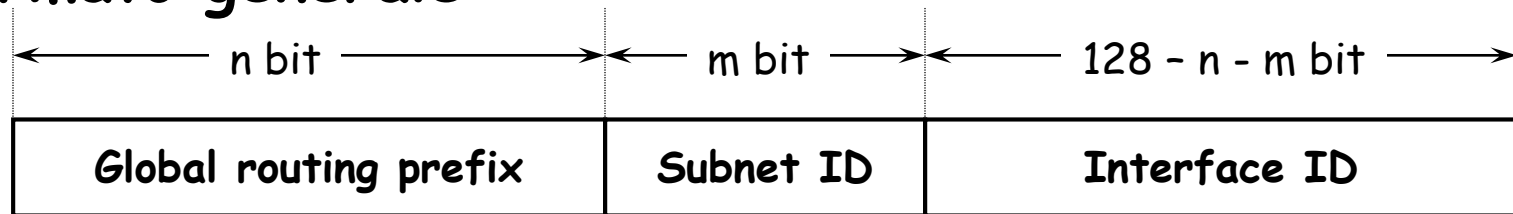
- Lo spazio degli indirizzi è organizzato ad albero mediante prefissi
 - *IPv6-address / prefix length*
- Tipi di indirizzi IPv6

Tipo di indirizzo	Prefisso (binario)	Notazione IPv6
Non specificato	000...0 (128 bit)	::/128
Loopback	000...1 (128 bit)	::1/128
Multicast	11111111	FF00::/8
Link-local Unicast	1111111010	FE80::/10
Site-local Unicast	1111111011	FEC0::/10
Global Unicast	Qualsiasi altro	



Indirizzi Global Unicast

■ Formato generale



■ Global Routing Prefix (n bit) (normalmente n=48)

- Identifica un sito complesso (un cluster di reti)

■ Subnet ID (m bit) (normalmente m=16)

- Identifica una specifica sottorete all'interno di un sito

■ Interface ID (128-n-m bit) (normalmente 64 bit)

- Identifica un'interfaccia fisica in una subnet
- Normalmente equivale all'indirizzo fisico dell'interfaccia
 - Indirizzo MAC a 64 bit



Indirizzi Speciali Unicast (1)

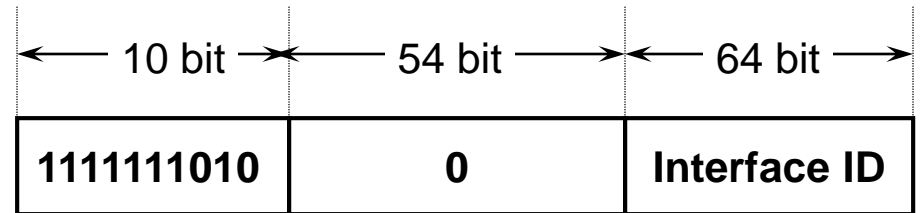
- L'indirizzo "Non Specificato" (0:0:0:0:0:0:0:0) indica l'assenza di un indirizzo
 - Non può essere assegnato ad un interfaccia fisica
 - È ad esempio utilizzato come source address nei pacchetti di richiesta di indirizzo nelle procedure di inizializzazione automatica degli host
 - Non può essere usato come Destination Address
- L'indirizzo "Loopback" (0:0:0:0:0:0:0:1) è utilizzato da un nodo per inviare un pacchetto a se stesso
 - Non può essere assegnato ad un interfaccia fisica
 - Non può essere usato come Source Address



Indirizzi Speciali Unicast (2)

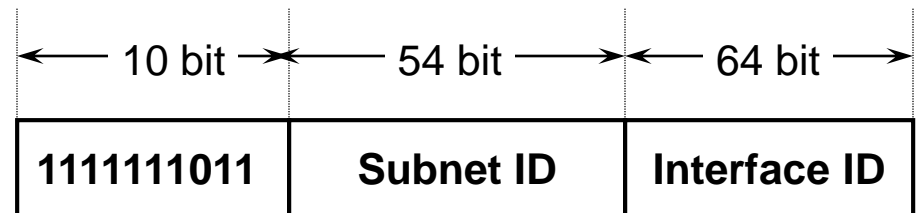
■ Indirizzi Link-local

- Prefisso: FE80::/10
- Possono essere usati solo sulla rete fisica alla quale è connessa l'interfaccia dell'host
- Servono a individuare gli host su un link
- Questi pacchetti non devono essere rilanciati da un router



■ Indirizzi Site-local

- Prefisso: FEC0::/10
- Equivalgono agli indirizzi privati IPv4 (es. 10.0.0.0)
- Possono essere usati solo all'interno di una Intranet





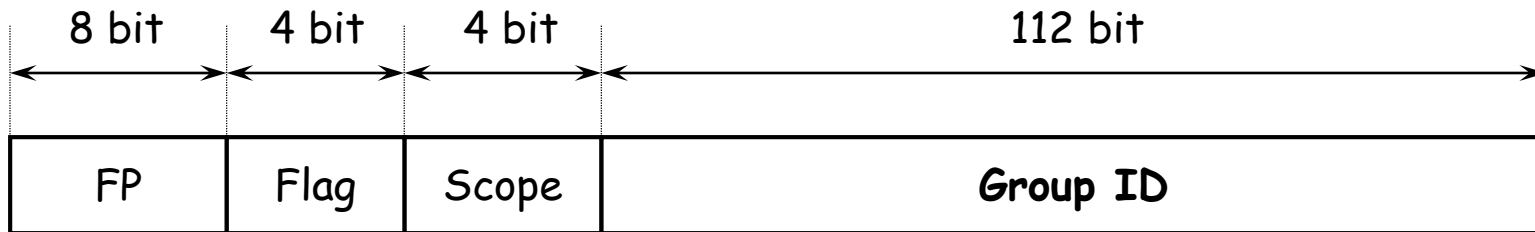
Indirizzi Anycast

- **Un indirizzo Anycast Identifica un insieme di interfacce**
 - Un pacchetto inviato ad un indirizzo di questo tipo è instradato verso l'interfaccia più vicina appartenente all'insieme
- **Gli indirizzi anycast sono ricavati all'interno dello spazio degli indirizzi unicast**
 - Sono indistinguibili dagli indirizzi unicast
 - I router devono essere configurati in modo da riconoscere tali indirizzi
- **Esempio:**
 - Possono essere utilizzati per identificare un insieme di router che appartengono ad uno stesso provider
 - Tale indirizzo può essere posto nel Routing extension header di un pacchetto IPv6 affinché raggiunga il provider



Indirizzi Multicast

□ Formato generale



■ Format Prefix (FP) (8 bit)

- 1111 1111

■ Flags (4 bit)

- 0000: indirizzo permanente
- 0001: indirizzo transitorio

■ Group ID (112 bit)

- Identifica il gruppo multicast

□ Scope (4 bit)

- Individua l'ambito di validità dell'indirizzo ovvero l'ambito in cui sono compresi i nodi appartenenti al gruppo multicast
- Esempi
 - 1: solo interfacce di un nodo
 - 2: solo nodi del link locale (link-scope)
 - 5: solo nodi del sito locale (site-scope)



Regole di allocazione degli indirizzi (1)

- Un indirizzo IPv6 può essere modellato come diviso in due campi
 - Network number (64 bit)
 - Host number (64 bit)
- Il problema è quello di individuare dei criteri per individuare il corretto spazio di indirizzi IPv6 da assegnare ad un singolo sito
 - Rete di un provider
 - Rete privata (intranet)
 - Postazioni d'utente (domestica, mobile, ecc.)
 - Singolo host



Regole di allocazione degli indirizzi (2)

■ Le regole adottate sono le seguenti:

- Prefisso /48 (16 bit di indirizzamento per le sottoreti) per un qualsiasi provider tranne quelli di grandi dimensioni
- Prefisso /64 nel caso in cui il sito è riconosciuto gestire solo una singola sottorete
- Prefisso /128 per un singolo dispositivo
- Ad un provider di grandi dimensioni può essere assegnato uno spazio delimitato da un prefisso più breve di 48 bit

■ Osservazioni

- Partizione dello spazio quasi statica
- Tutte le reti hanno lo stesso spazio di indirizzamento (16 bit di identificativo di sottorete e 64 bit di identificatore di host)
- Una rete mobile (veicolo o un terminale con interfacce multiple) ha la possibilità di gestire una molteplicità di dispositivi terminali
- Un PC che si connette alla rete riceve un singolo indirizzo



Marco Listanti

IPv6: Autoconfigurazione



Generalità (1)

- **Il processo di autoconfigurazione permette ad un host di**
 - Creare il proprio link-local address e verificarne l'univocità
 - Determinare la sottorete a cui appartiene e quindi il proprio prefisso
- **Stateless autoconfiguration**
 - Non è necessaria la presenza di un server
 - L'indirizzo di un host viene individuato sulla base di due informazioni
 - Identificatore di interfaccia (disponibile localmente)
 - Identificatore di sottorete (comunicato da un router)
 - Non permette di controllare l'assegnazione degli indirizzi in un sito
- **Stateful autoconfiguration**
 - L'host riceve le informazioni di configurazione da un server
 - Permette di controllare strettamente il processo di assegnazione degli indirizzi



Generalità (2)

- Ogni indirizzo è caratterizzato da un tempo di validità (*lifetime*)
 - Infinito (assegnazione permanente)
 - Finito (assegnazione dinamica)
- Se il tempo di validità scade, l'associazione tra indirizzo e host non è più valida e l'indirizzo può essere riassegnato ad un altro host
- L'unicità di un indirizzo è garantita da un algoritmo di rivelazione di indirizzi duplicati (*Duplicated Address Detection Algorithm*)
 - L'algoritmo è eseguito in entrambe le procedure stateless o stateful prima di utilizzare l'indirizzo assegnato



Stateless Autoconfiguration (1)

- Evita la configurazione manuale di un host
- Permette ad un host di ottenere un indirizzo unico per ognuna delle sue interfacce
 - Si suppone che ogni interfaccia sia caratterizzata da un identificatore predefinito e unico
- Evita la presenza di un server di configurazione in siti di piccola e media dimensione
 - Un host può determinare automaticamente il prefisso associato alla rete a cui è connesso
- Facilita l'eventuale rinumerazione della rete in caso di cambio di provider



Stateless Autoconfiguration (2)

- Una procedura di Stateless Autoconfiguration (SA) può essere eseguita solo su una rete multicast (es. LAN)
- Procedura
 - Inizia al momento dello startup di un host
 - Viene generato il link-local address per l'interfaccia (prefisso FE80::/10)
 - Viene inviato sulla rete un messaggio di "*Neighbor Solicitation*" contenente il nuovo indirizzo per verificarne l'unicità
 - Se un nodo risponde negativamente la procedura di autoconfigurazione è bloccata
 - Viene inviato un messaggio "*Router Solicitation*" per ottenere dal router l'indicazione del prefisso di rete per la formazione degli indirizzi *site-local address* e *global address*
 - Un router emette i messaggi "*Router Advertisements*" per rispondere alla richiesta del nodo
 - I messaggi "*Router Advertisements*" sono comunque emessi periodicamente per consentire le operazioni di verifica e di aggiornamento degli indirizzi



Stateful Autoconfiguration

- Permette la configurazione automatica di un host con l'ausilio di un server
- Il protocollo di colloquio tra Host e Server è denominato *Dynamic Host Configuration Protocol IPv6 (DHCPv6)*
 - È un estensione del protocollo DHCP utilizzato in IPv4
- DHCPv6 sfrutta i meccanismi specifici di IPv6 e ha le seguenti caratteristiche
 - Un host usa il proprio link-local address per comunicare con il DHCP server
 - Ha la possibilità di fornire una molteplicità di indirizzi per una interfaccia
 - I messaggi sono contenuti in pacchetti IPv6
 - Rende possibili cambi di configurazione automatici



Protocollo DHCPv6

- I messaggi DHCPv6 sono trasferiti tramite il protocollo UDP
- Un DHCPv6 server riceve messaggi da un client mediante indirizzi multicast di tipo link-scope
- Sono possibili meccanismi di relay per consentire l'accesso a DHCPv6 server anche non residenti sullo stesso link del client



Messaggi DHCPv6 (1)

■ Solicit

- È emesso da un client per localizzare un DHCPv6 server

■ Advertise

- È emesso da un server in risposta ad un messaggio *Solicit* per indicare che è disponibile un servizio DHCPv6

■ Request

- È emesso da un client per richiedere ad uno specifico server DHCPv6 l'assegnazione di un indirizzo e i relativi parametri di configurazione

■ Confirm

- È emesso da un client verso qualsiasi server per verificare che l'indirizzo assegnato è valido sul link a cui il client è connesso



Messaggi DHCPv6 (2)

■ Renew

- È emesso da un client verso il server che ha eseguito l'assegnazione per estendere il lifetime della configurazione stessa

■ Rebind

- È emesso da un client verso qualsiasi server, dopo aver ricevuto la risposta ad un messaggio Renew, per comunicare l'estensione del lifetime della configurazione stessa

■ Replay

- È emesso da un server in risposta ai messaggi Solicit, Request, Renew, Rebind e contiene gli indirizzi assegnati e i parametri di configurazione

■ Release

- È emesso da un client verso il server che ha eseguito l'assegnazione per indicare il rilascio di uno o più indirizzi



Messaggi DHCPv6 (3)

■ Decline

- È emesso da un client verso il server che ha eseguito l'assegnazione per indicare che uno o più indirizzi non sono validi perché già in uso

■ Reconfigure

- È emesso da un server per informare i client che deve essere iniziata una procedura di variazione nei parametri di configurazione tramite l'invio di messaggi di *Renew* o *Information-Request*

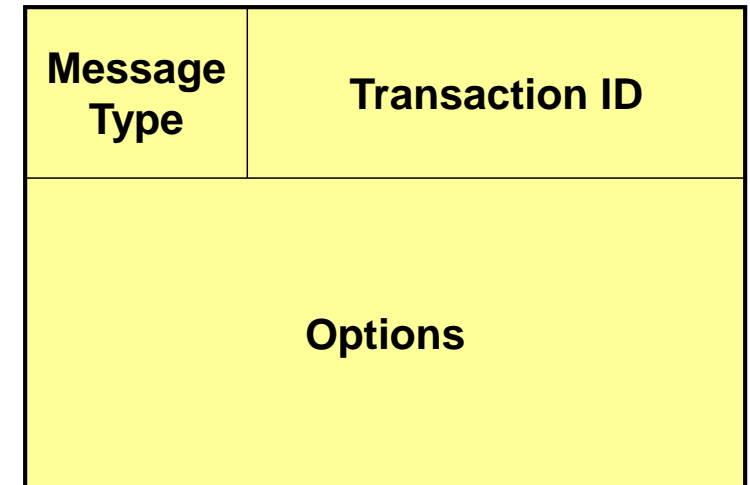
■ Information-Request

- È emesso da un client verso un server per richiedere i parametri di configurazione, ma non l'assegnazione di un indirizzo



Formato Messaggi DHCPv6 (1)

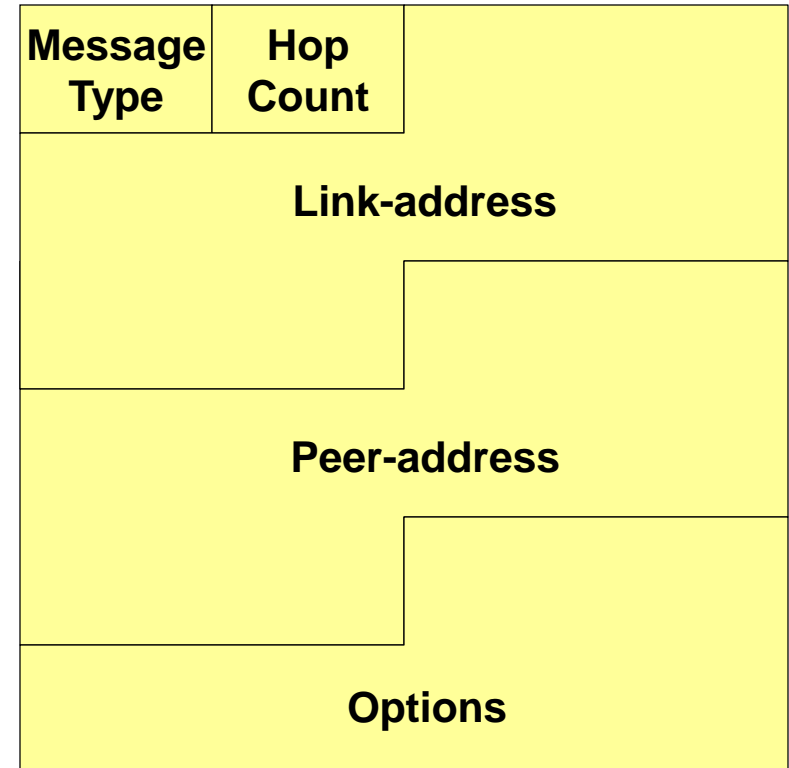
- Tutti i messaggi DHCPv6 emessi da un client hanno lo stesso formato dell'header
- **Message Type (8 bit)**
 - Identifica il tipo di messaggio
- **Transaction ID (24 bit)**
 - Identifica la transazione client-server a cui si riferisce il messaggio
- **Options (lunghezza variabile)**





Formato Messaggi DHCPv6 (2)

- Tutti i messaggi DHCPv6 emessi da un server hanno lo stesso formato dell'header
- **Message Type (8 bit)**
 - Identifica il tipo di messaggio
- **Hop-count (8 bit)**
 - Numero di relay node che hanno rilanciato il messaggio
- **Link address (128 bit)**
 - Global address o site-local address
- **Peer address (128 bit)**
 - Indirizzo del client
- **Options (lunghezza variabile)**





Marco Listanti

Strategie di transizione da IPv4 a IPv6



Generalità (1)

- La transizione da IPv4 a IPv6 deve necessariamente prevedere un intervallo di tempo (anche molto lungo) in cui i due protocolli coesisteranno in rete
- È indispensabile definire dei meccanismi che assicurino
 - la compatibilità tra sistemi che supportano le due versioni del protocollo
 - La possibilità di una migrazione graduale senza degradazione del servizio offerto da Internet
- I meccanismi che sono stati definiti identificano le modalità di funzionamento dei router IPv6 quando devono interlavorare con i router IPv4 o utilizzano un'infrastruttura IPv4



Generalità (2)

■ I meccanismi definiti sono:

■ Dual IP layer (Dual stack)

- Fornisce il supporto completo di entrambe le versioni del protocollo in un router

■ Indirizzi IPv4 immersi (embedded) nella struttura IPv6

- Strutture di indirizzi IPv6 che contengono indirizzi IPv4

■ Configurazione di tunnel IPv6 in IPv4

- Configurazione amministrativa di tunnel punto-punto tra router IPv6 attraverso reti IPv4
- I pacchetti IPv6 sono incapsulati in pacchetti IPv4

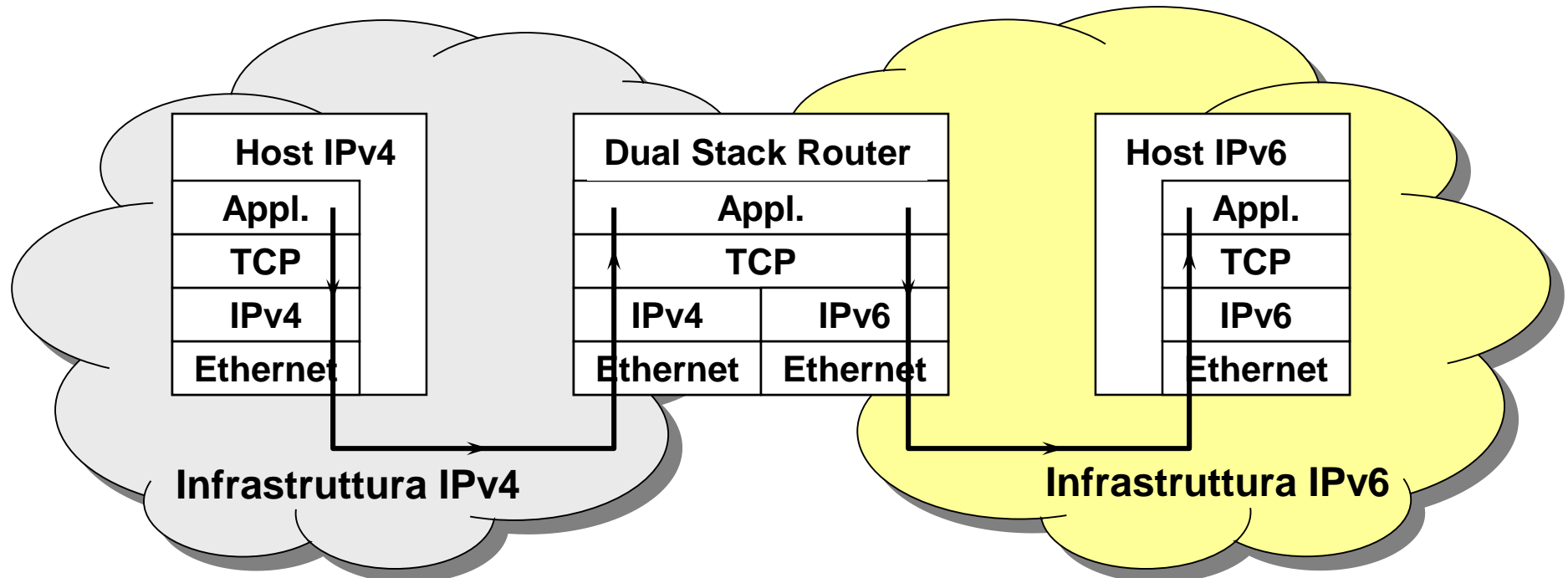
■ Tunnel automatico di IPv6 in IPv4

- Creazione automatica di tunnel IPv6 attraverso reti IPv4 mediante l'uso degli indirizzi IPv4 contenuti negli indirizzi IPv4-compatibili



Dual Stack

- Un nodo gestisce entrambi le versioni del protocollo
- È il modo più diretto per mantenere la compatibilità tra due sezioni di rete utilizzanti le due versioni del protocollo



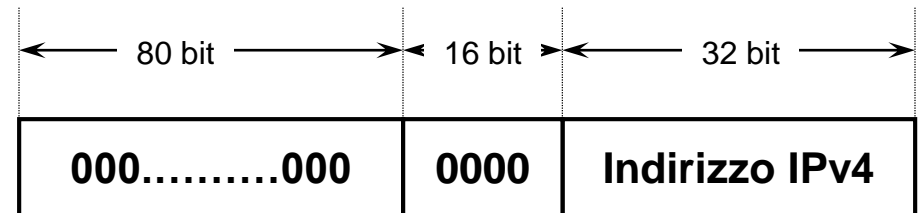


Indirizzi IPv4 immersi (embedded)

□ Sono definite tre tipologie

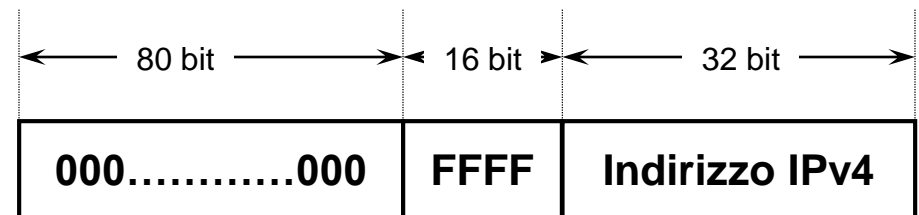
■ IPv4-compatible address

- 0::0:a:b:c:d
- Sono utilizzati quando è necessario effettuare tunnel di pacchetti IPv6 attraverso reti IPv4



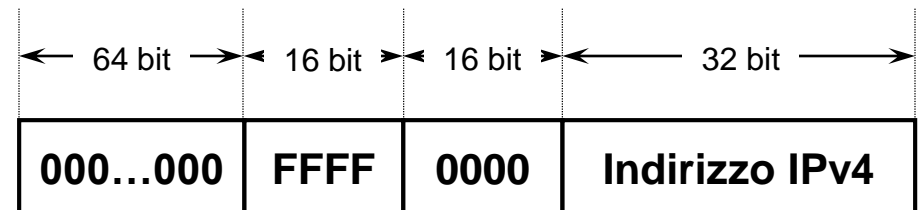
■ IPv4-mapped IPv6 address

- 0::ffff:a:b:c:d
- Sono utilizzati da nodi IPv6 per indirizzare nodi che supportano solo il protocollo IPv4



■ IPv4-translated IPv6 address

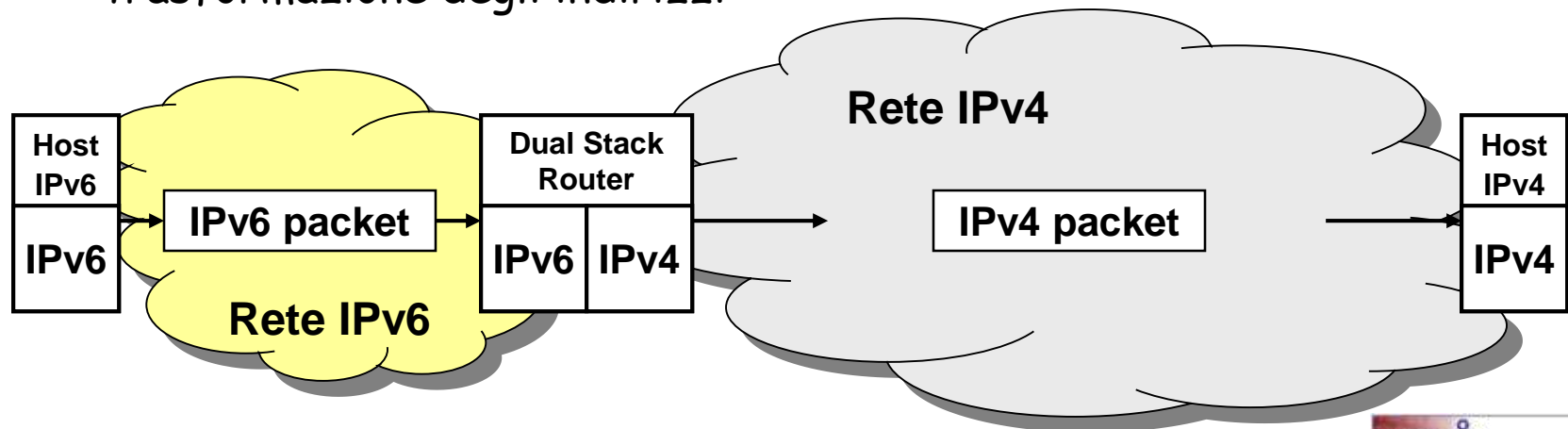
- 0:ffff:0:a:b:c:d
- Identificano un host IPv6 quando questi comunica con un nodo IPv4





Esempio

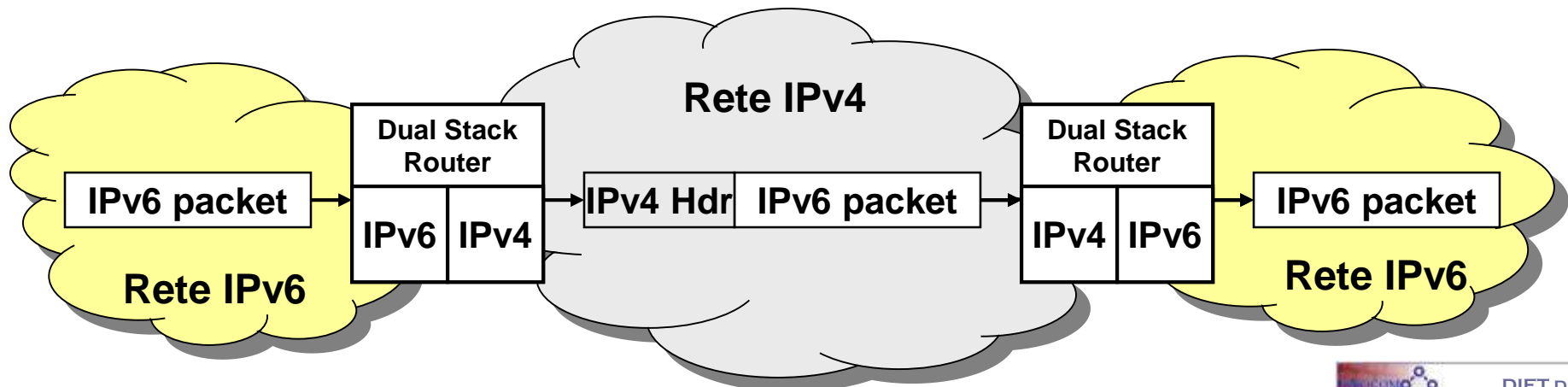
- **Host IPv6 in comunicazione con un Host IPv4**
 - Si assume che all'host IPv6 sia assegnato un indirizzo IPv4-translated (meccanismo da definire)
 - Nel pacchetto IPv6 sono contenuti gli indirizzi
 - IPv4-mapped dell'host IPv4
 - IPv4-translated dell'host IPv6
 - Il router dual stack provvederà alla conversione dei protocolli e alla trasformazione degli indirizzi





Tunnelling (1)

- La rete IPv6 si svilupperà a isole all'interno della rete IPv4 esistente
- Il meccanismo del Tunnelling consente di connettere aree IPv6 attraverso un'infrastruttura IPv4
- La presenza di un payload IPv6 in un pacchetto IPv4 è indicata dal valore del campo Protocol uguale a 41





Tunnelling (2)

■ Sono possibili diverse modalità di tunnelling

■ Router to Router

- Due router IPv6/IPv4 sono interconnessi da un tunnel IPv4
- Il tunnel è un segmento intermedio del cammino end-to-end IPv6

■ Host to Router

- Un Host IPv6/IPv4 può accedere ad un router IPv6/IPv4 tramite una rete IPv4
- Il tunnel è il primo segmento del cammino end-to-end IPv6

■ Host to Host

- Due host IPv6/IPv4 sono interconnessi da un tunnel IPv4
- Il tunnel coincide con l'intero cammino end-to-end IPv6

■ Router to Host

- Un Router IPv6/IPv4 è connesso all'host finale IPv6/IPv4 tramite una rete IPv4
- Il tunnel è l'ultimo segmento del cammino end-to-end IPv6



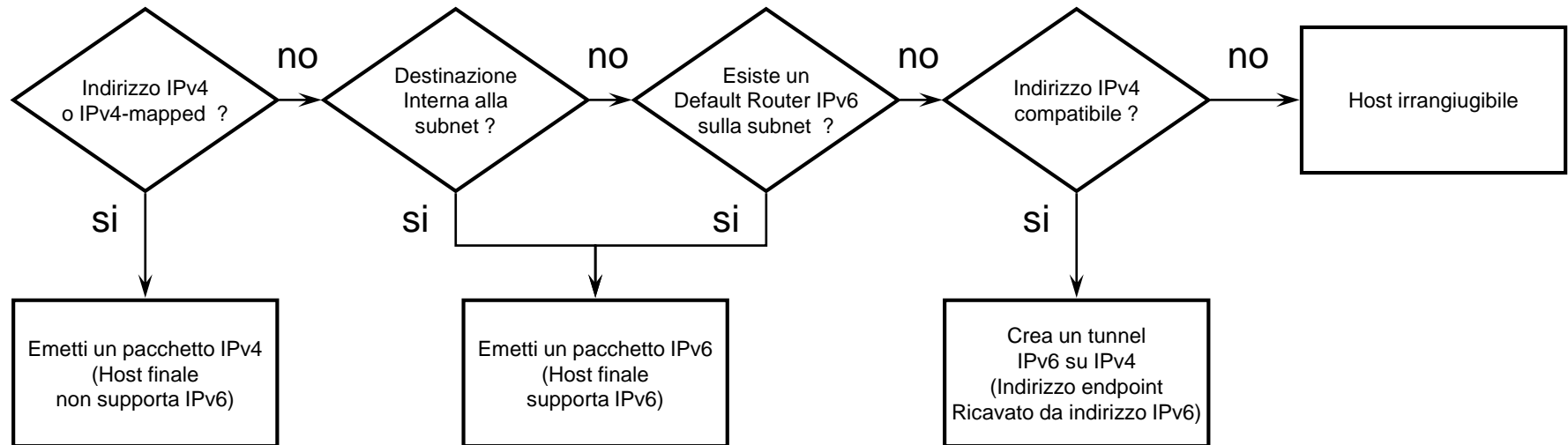
Tunnelling (3)

- Le modalità di tunnelling si differenziano in base al meccanismo con cui il nodo che effettua l'incapsulamento del pacchetto determina l'indirizzo del nodo terminale del tunnel (Endpoint)
- ***Tunnel configurati***
 - L'endpoint del tunnel è un router e quindi la destinazione finale del pacchetto non coincide con l'endpoint del tunnel
 - L'indirizzo IPv6 contenuto nel pacchetto non identifica l'indirizzo IPv4 dell'endpoint del tunnel
 - Tale informazione deve essere resa disponibile tramite configurazione
- ***Tunnel automatici***
 - L'endpoint del tunnel è un host e quindi la destinazione finale del pacchetto coincide con l'endpoint del tunnel
 - E' indispensabile utilizzare un indirizzo IPv6 che identifica automaticamente anche l'indirizzo IPv4 dell'endpoint del tunnel (indirizzi IPv4-compatibili)



Tunnel automatici (1)

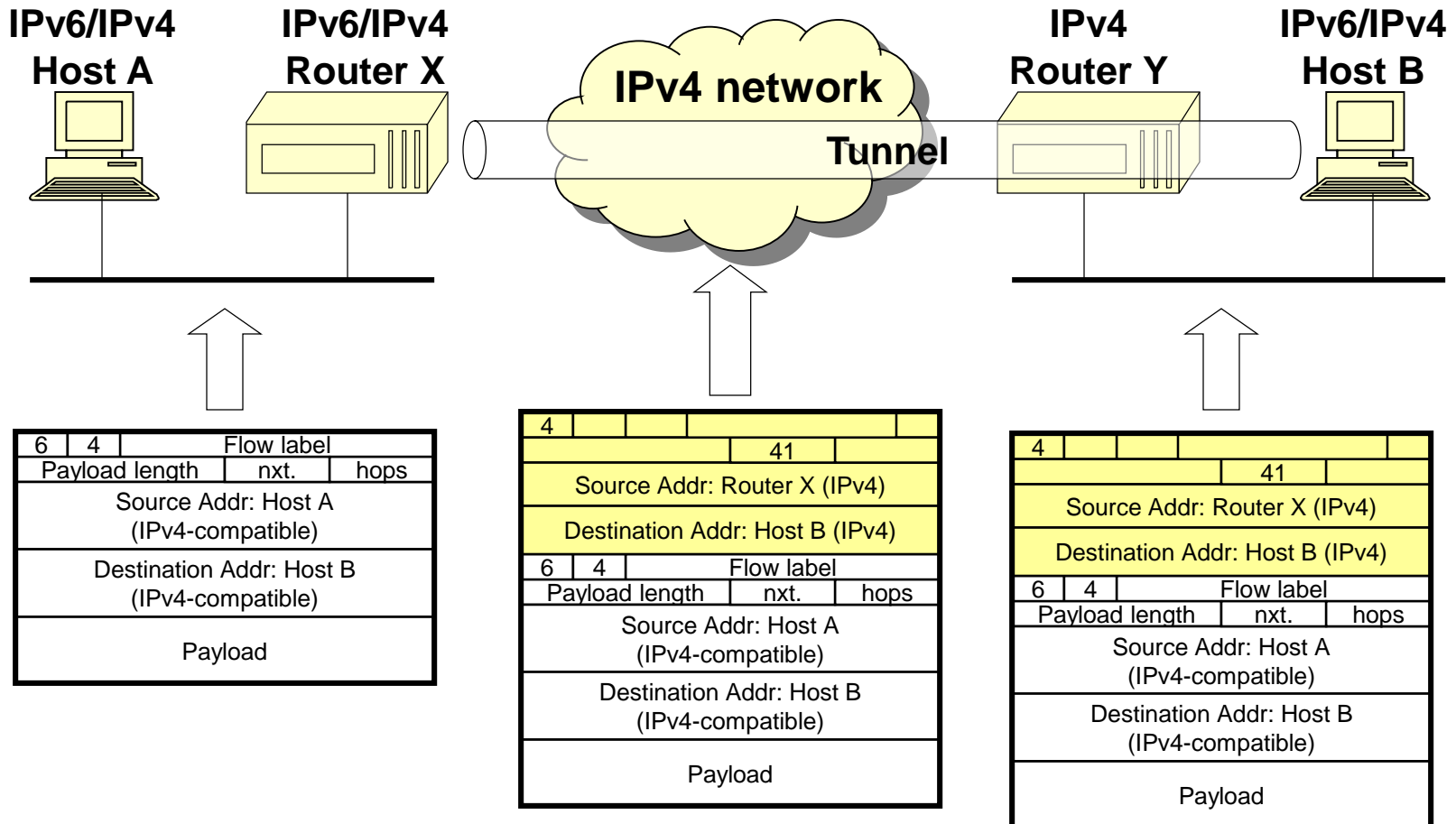
■ Algoritmo di decisione sull'effettuazione di un Tunnel automatico



■ L'algoritmo privilegia l'uso dell'infrastruttura IPv6 se esiste

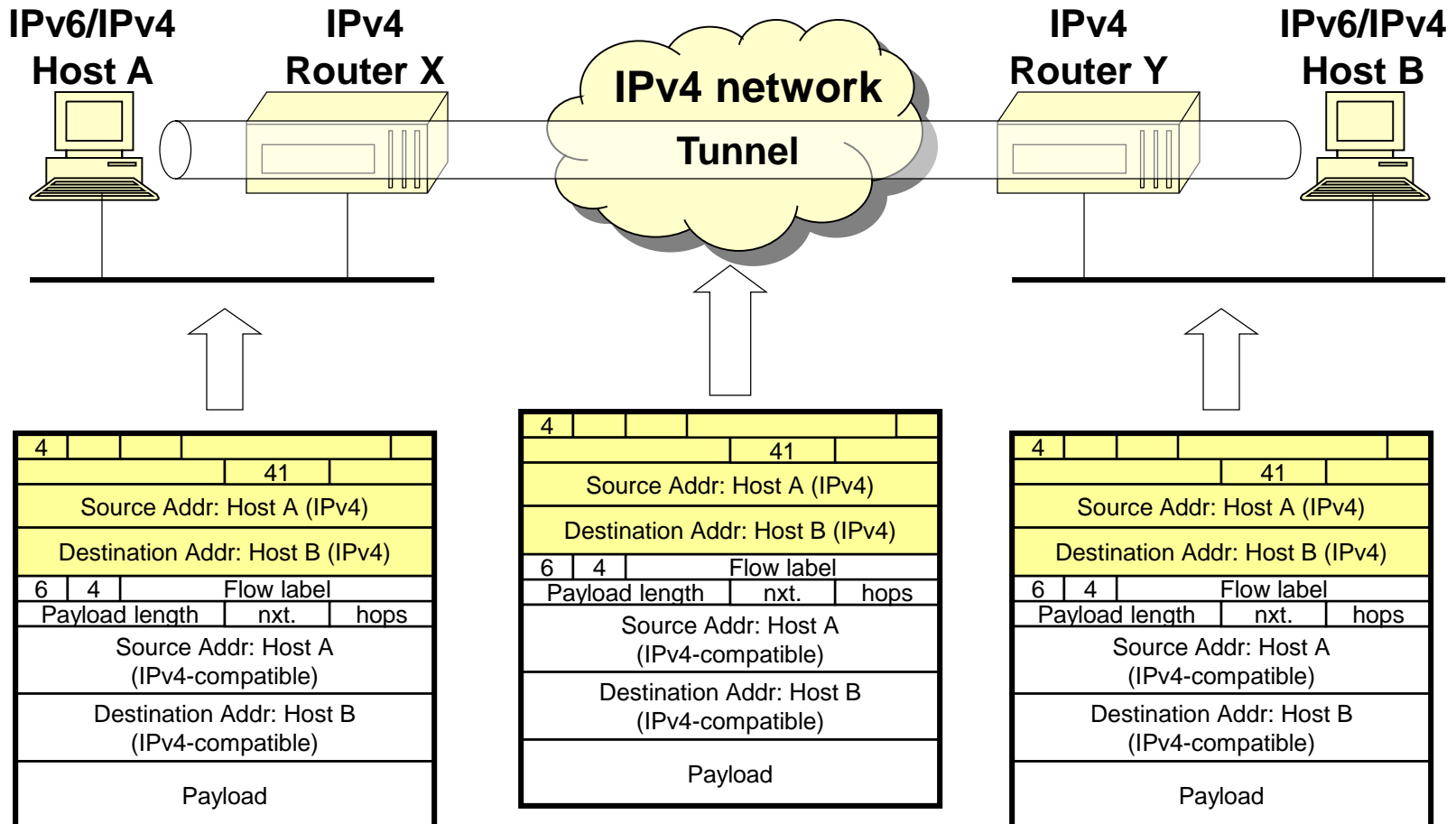


Tunnel automatico router-to-host





Tunnel automatico host-to-host





Tunnel configurati router-to-router

