



Protocollo IPv6

IPv6

- IP (v4) e' stato un grande successo
- Perche' cambiare
 - ◆ Spazio di indirizzamento limitato
 - ◆ Spazio di indirizzamento assegnato in modo non uniforme
 - ◆ Funzioni non presenti nel progetto originario
 - Real time
 - Sicurezza
- Perche' IPv6
 - ◆ Frutto di confusione



IPv6 Funzionalità

IPv6 – funzionalità 1/2

- Aumento dello spazio di Indirizzamento
 - ◆ Indirizzi a 128 bit
 - ◆ Indirizzamento gerarchico basato sul concetto di prefisso
- Indirizzamento gerarchico
- Semplificazione della struttura dell'header del pacchetto
- Intestazione di formato variabile
 - ◆ In realta' anche in IPv4 (teoricamente)
- Protocollo estendibile
- Supporto per l'autoconfigurazione
- Supporto per l'assegnazione delle risorse
 - ◆ Astrazione di flusso
 - ◆ Servizi differenziati

IPv6 – funzionalità 2/2

- Le funzioni ed il formato del pacchetto di 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 UnicastAddress Format
 - ◆ **RFC 3177:** IAB/IESG Recommendations on IPv6 AddressAllocations to Sites
 - ◆ **RFC 2461:** NeighborDiscoveryforIP version6 (IPv6)
 - ◆ **RFC 2462:** IPv6 statelessaddressautoconfiguration
 - ◆ **RFC 2893:** Transition mechanism forIPv6 hosts and routers
 - ◆ **RFC 3056:** Connection of IPv6 domains via IPv4 clouds
 - ◆ **RFC 3315:** Dynamic Host Configuration Protocol for IPv6 (DHCPv6)

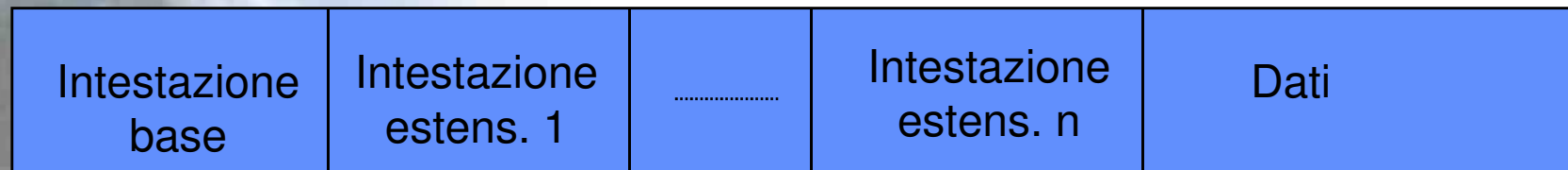


IPv6

Formato del Pacchetto

Formato generale del pacchetto IPv6

- Intestazione di base obbligatoria
 - ◆ Contiene le informazioni comuni a tutti i datagrammi
- 0 o piu' intestazioni opzionali
 - ◆ Servizi opzionali
- Payload
 - ◆ Sono i bit informativi



Opzionali

Intestazioni

- Intestazione base

- ◆ Contiene informazioni generali sul pacchetto

- Indirizzi sorgente
 - Indirizzo destinazione
 -

- Intestazioni di estensione

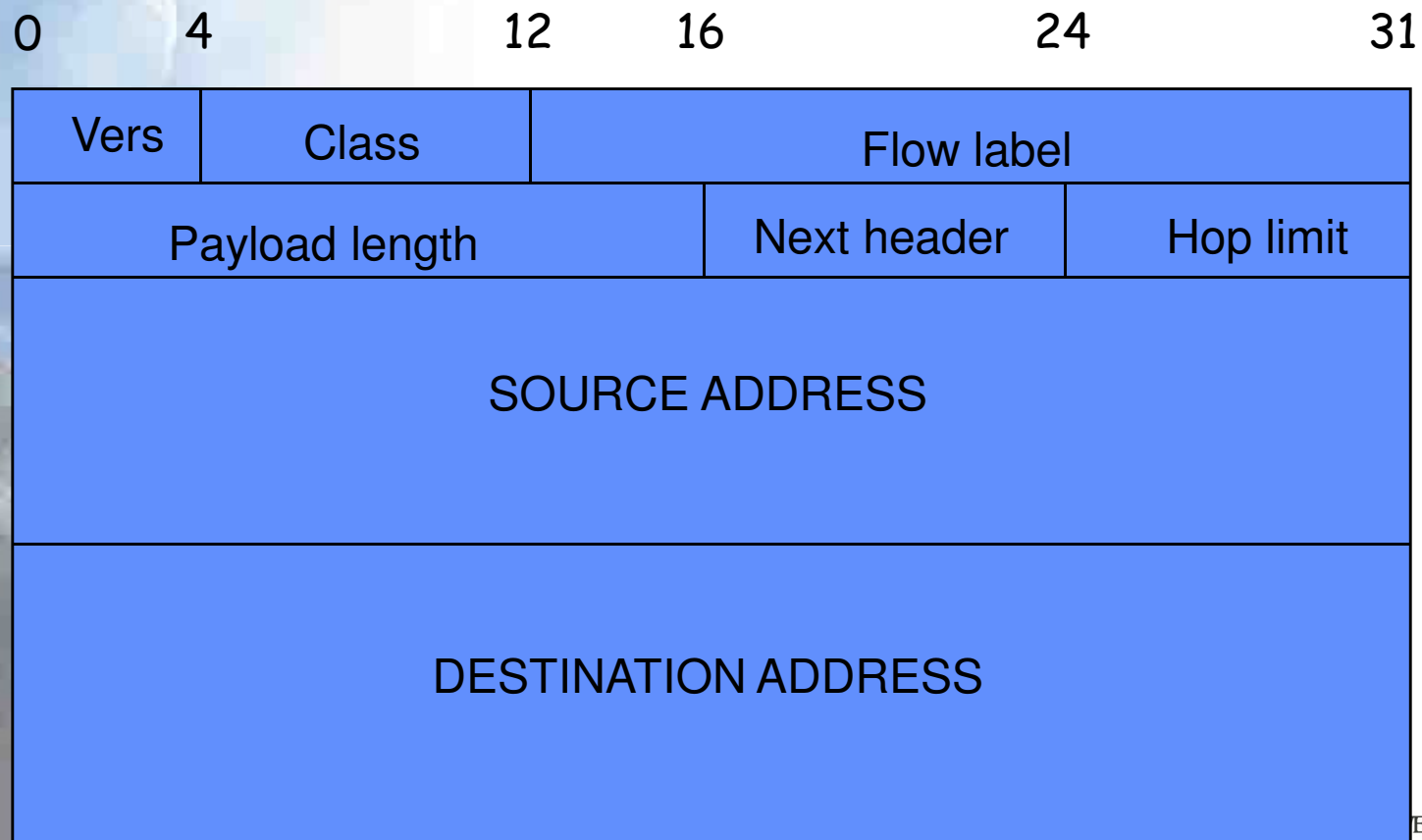
- ◆ Servono a implementare servizi specifici

- Opzioni

- ◆ Servono a implementare servizi aggiuntivi o nuove funzionalita'

Intestazione di base 1/3

- Lunghezza costante
 - ◆ Info su frammentazione spostata



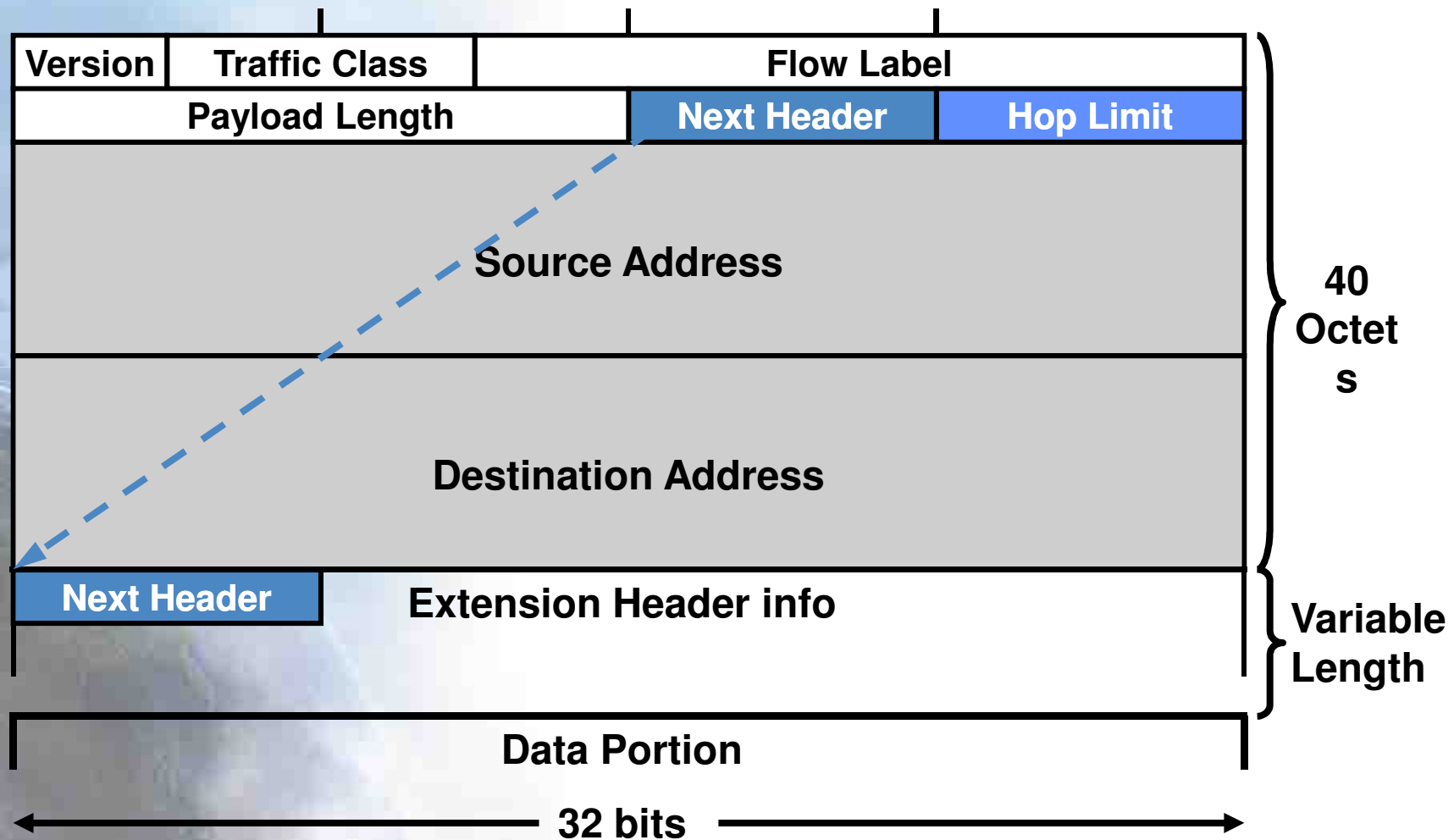
Intestazione di base 2/3

- Version: 4 bit.
 - ◆ 6 IPv6.
- Traffic Class: 8 bit.
 - ◆ Valore per identificare la priorit  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 pu  modificare questo campo per tutti i pacchetti in uscita verso altre reti, al fine di assegnare una classe di servizio concordata con altri ISP
- Flow Label: 20 bit
 - ◆ Uso ancora non chiaro. Usato un flusso
 - ◆ Pacchetti appartenenti allo stesso flusso avranno:
 - Stesso indirizzo IPv6 sorgente
 - Stesso indirizzo IPv6 destinazione
 - Stesso valore del campo flow-label

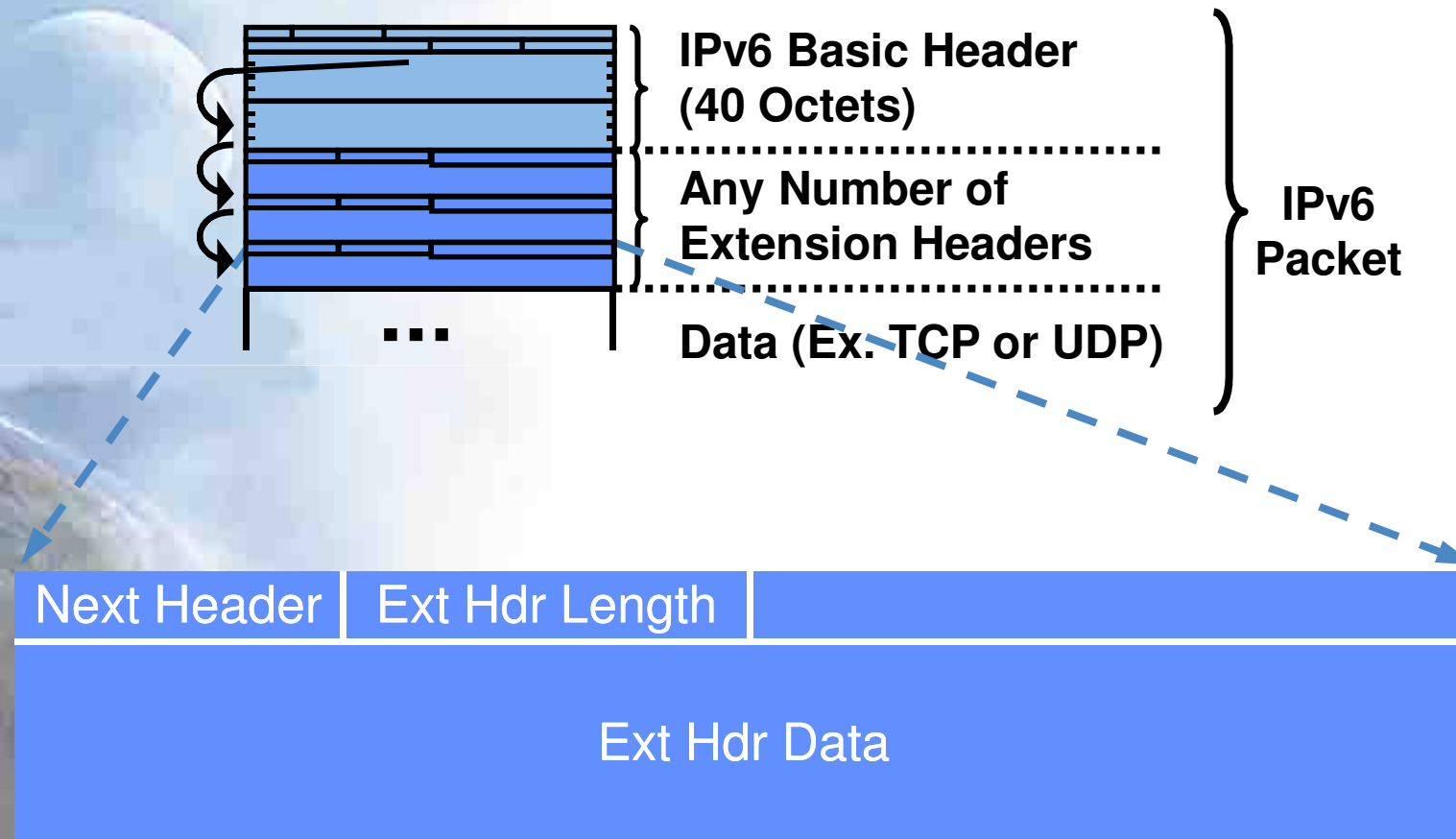
Intestazione di base 3/3

- 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
- Next Header: 8 bit
 - ◆ Specifica l'header successivo
 - ◆ Se è un protocollo di livello più alto, i valori sono compatibili con quelli IPv4
- Hop Limit: 8 bit
 - ◆ Sostituisce TTL IPv4

IPv6 Header Format: Next Header



Extension Headers

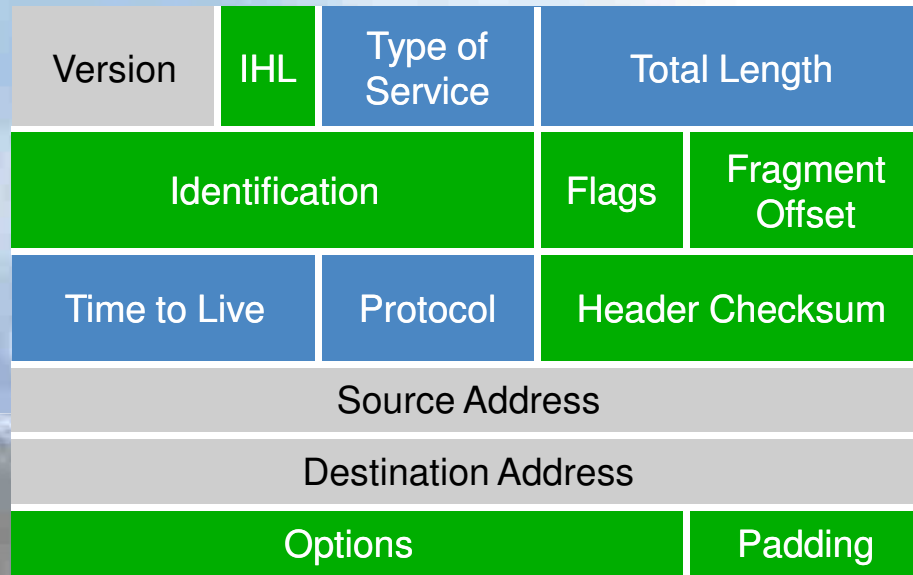


Intestazioni di estensione

- Ciascuna serve a implementare un meccanismo diverso
- Esempi:
 - ◆ Autenticazione
 - ◆ Frammentazione/deframmentazione
 - ◆ Instradamento
 - ◆
- Ogni datagramma contiene soltanto le intestazioni necessarie

IPv4 vs IPv6 Header

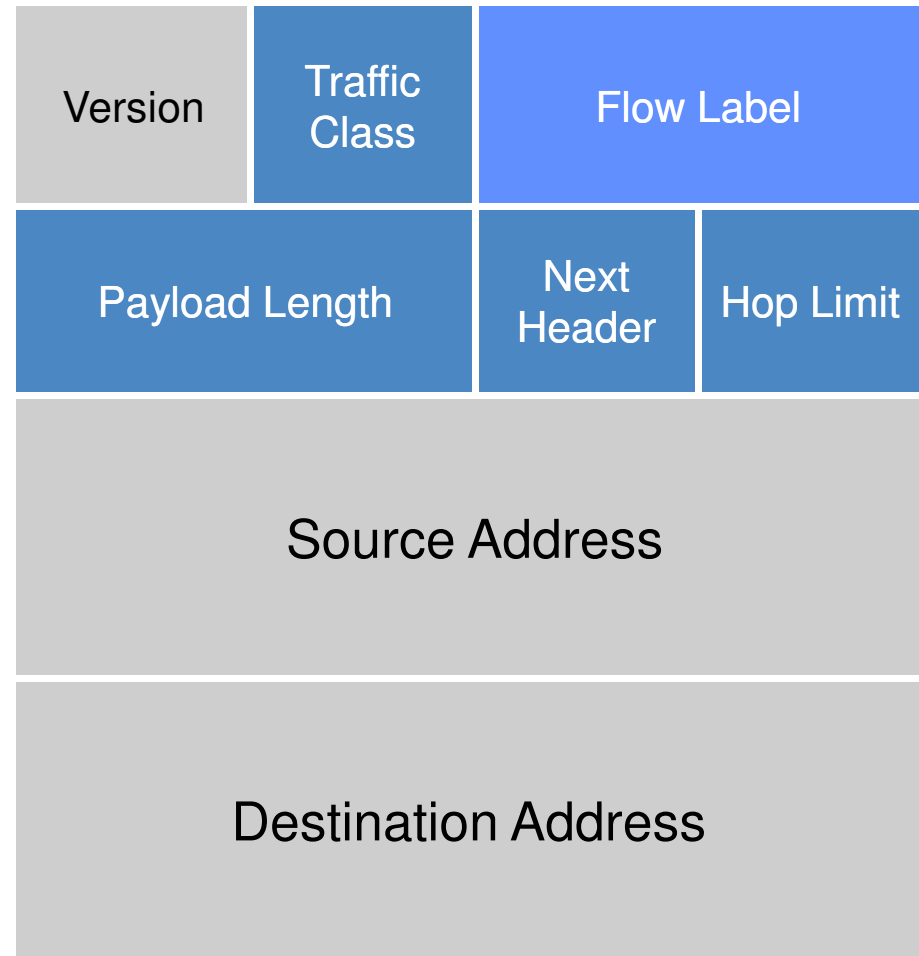
IPv4 Header



Legend

- Field's Name Kept from IPv4 to IPv6
- Fields Not Kept in IPv6
- Name and Position Changed in IPv6
- New Field in IPv6

IPv6 Header



IPv6 Header Options (RFC 2460)

IPv6 Header
Next Header
= TCP

TCP Header
+ Data

IPv6 Header
Next Header
= Routing

Routing Header
Next Header
= TCP

TCP Header
+ Data

IPv6 Header
Next Header
= Routing

Routing Header
Next Header
= Fragment

Fragment Header
Next Header
= TCP

Fragment of
TCP Header
+ Data

- Processed only by node identified in IPv6 destination address field => much lower overhead than IPv4 options
 - ◆ Exception: hop-by-hop options header
- Eliminated IPv4's 40-octet limit on options
 - ◆ In IPv6, limit is total packet size, or path MTU in some cases

Esempio

- Route serve per l'instradamento
- Auth serve per servizi di autenticazione
- TCP indica che la porzione che segue contiene un segmento TCP (i dati del datagram IPv6)
- Router esaminano solo alcune intestazioni di estensione

Intestazione Base Next = Route	Intestazione Route Next = Auth	Intestazione Auth Next = TCP	Segmento TCP (Dati)
--------------------------------------	--------------------------------------	------------------------------------	---------------------

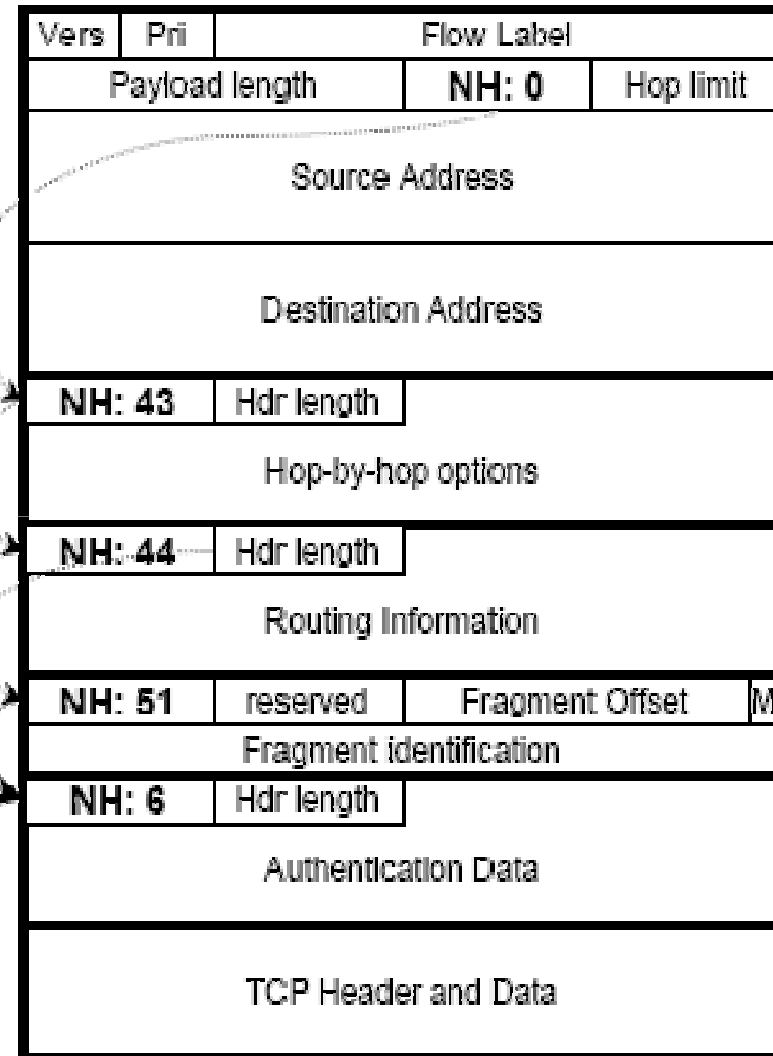
Alcuni header 1/2

- Nel next header sono contenuti i codici che identificano l'header che segue nel pacchetto
- Sono riportati alcuni tipi di extension header

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

Alcuni header 2/2

- 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



Extension Header

L'ordine di inserimento degli EH nel pacchetto è il seguente

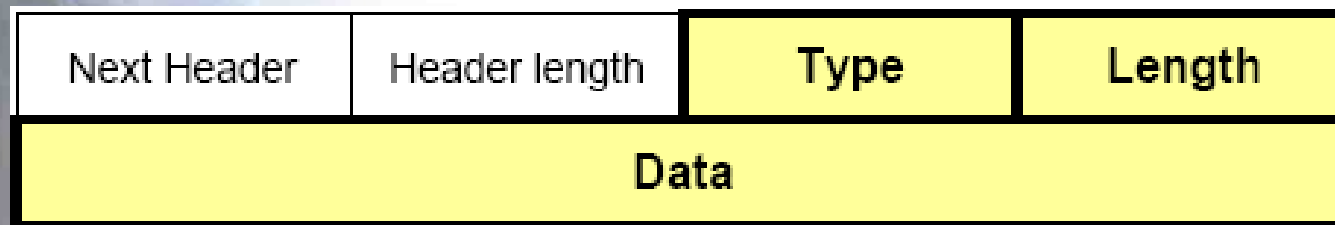
- ◆ **•IPv6 header**
- ◆ **•Hop-by-hop options header**
- ◆ **•Destination options header**
 - –opzioni che devono essere elaborate dal nodo che appare nel campo DestinationAddress e, successivamente, dalle seguenti destinazioni indicate nel Routing header
- ◆ **•Routing header**
- ◆ **•Fragment header**
- ◆ **•Authentication header**
- ◆ **•Encapsulating Security Payload header**
- ◆ **•Destination Options header**
 - –Opzioni che devono essere elaborate dal nodo destinazione finale
- ◆ **•Upper-layer header**

Opzioni IPv6

- IPv6 permette di definire intestazioni per ulteriori opzioni
- Permettono estensioni future del protocollo
- Estensioni salto-salto
 - ◆ Devono essere elaborate da ogni router intermedio
- Estensioni punto-punto
 - ◆ Elaborate soltanto a destinazione

Hop-by-Hop Options Header 1/3

- 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



Hop-by-Hop Options Header 2/3

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

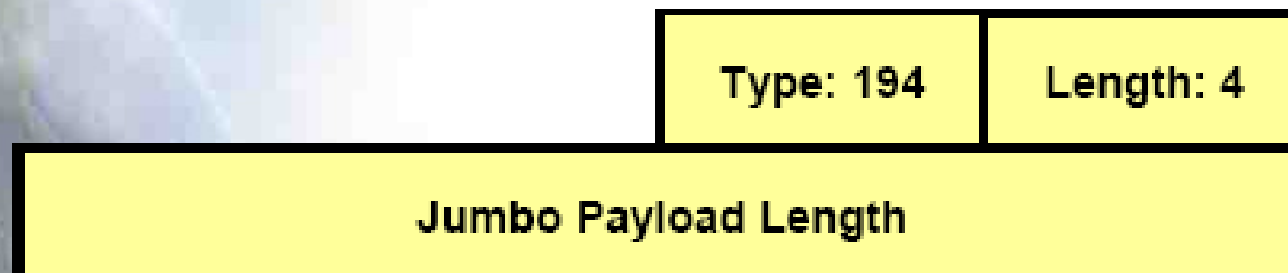
Type	Action
00xxxxxx	Ignora l'opzione e elabora ugualmente il datagramma
01xxxxxx	Scarta il datagramma
10xxxxxx	Scarta il datagramma ed invia un messaggio ICMP
11xxxxxx	Scarta il datagramma ed invia un messaggio ICMP solo se la destinazione non è multicast

- Il terzo bit stabilisce se il campo value può essere modificato

Type	Action
xx0xxxxx	Il campo value non deve essere modificato
xx1xxxxx	Il campo value può essere modificato

Hop-by-Hop Options Header 3/3

- 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



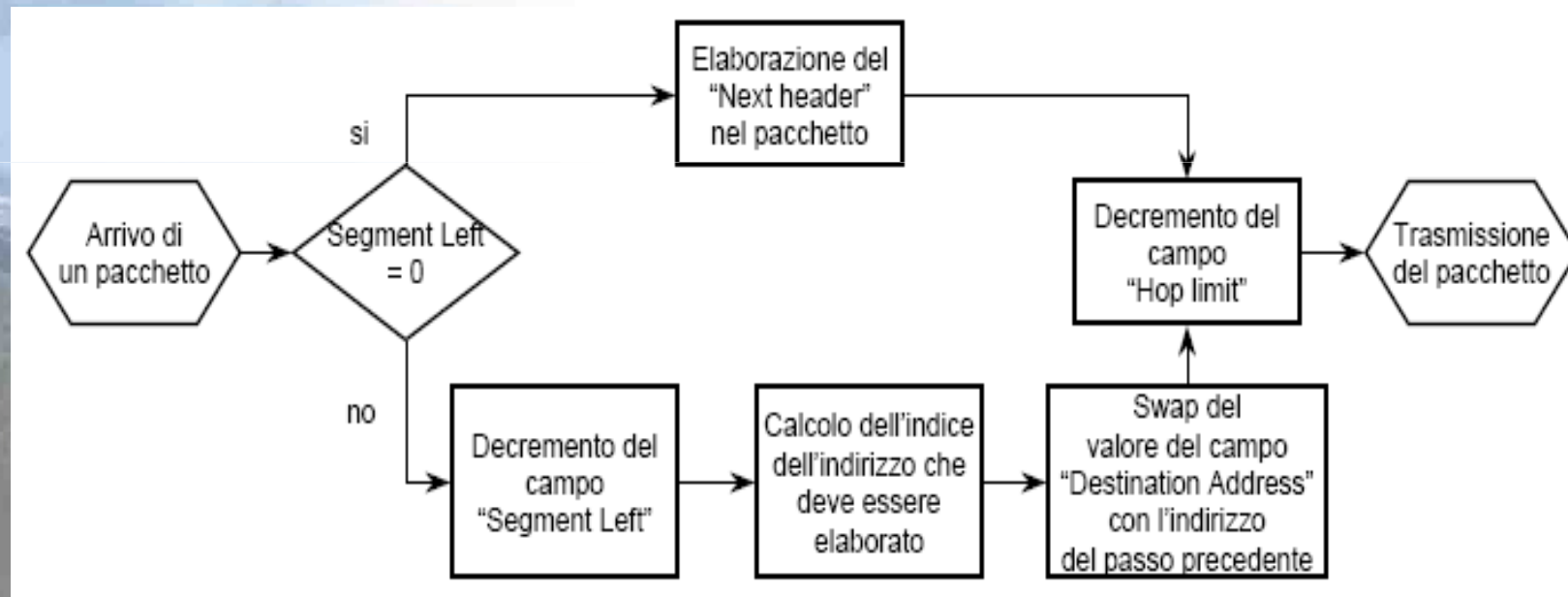
Routing Header 1/3

Next Header	Hdr Length	Type: 0	Segment Left
Reserved	Strict/Loose Bit Mask		
Address [0]			
Address [1]			
.....			
Address [n-1]			

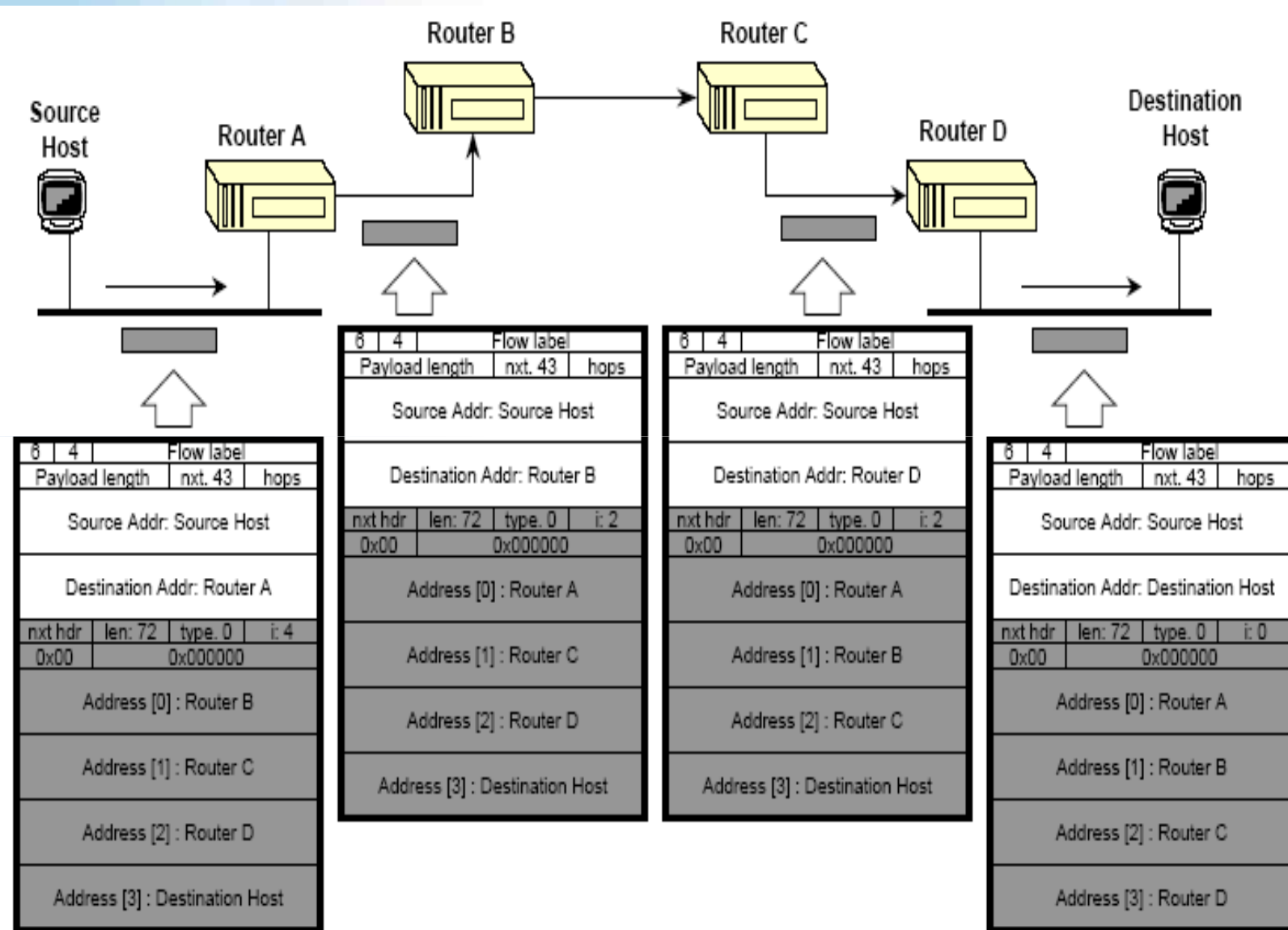
- Permette l'instradamento di un pacchetto su un cammino predefinito
- Fornisce ai router indicazioni per l'instradamento del datagramma
- Segment left (8 bit)•
 - ◆ indica il numero di indirizzi che devono essere ancora elaborati
 - ◆ ogni router decrementa tale campo
- Strict/Loose bit mask•
 - ◆ indica, per ogni indirizzo della lista, le modalità di instradamento
 - 0 : instradamento diretto obbligatorio
 - 1 : possibile instradamento attraverso router intermedi

Routing Header 2/3

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



Routing Header 3/3



Fragment Header 1/2

- Il nodo sorgente determina il valore della MTU che deve essere rispettato dai pacchetti lungo il cammino
- Se un pacchetto ha dimensione maggiore della MTU, il nodo sorgente esegue la frammentazione del pacchetto
- Tutti i frammenti hanno lunghezza multipla di 8 bytes

Next Hdr	Reserved	Fragment Offset	0	M
Fragment Identification				

◆ FragmentOffset

- specifica la posizione del primo byte del frammento nel datagramma originale

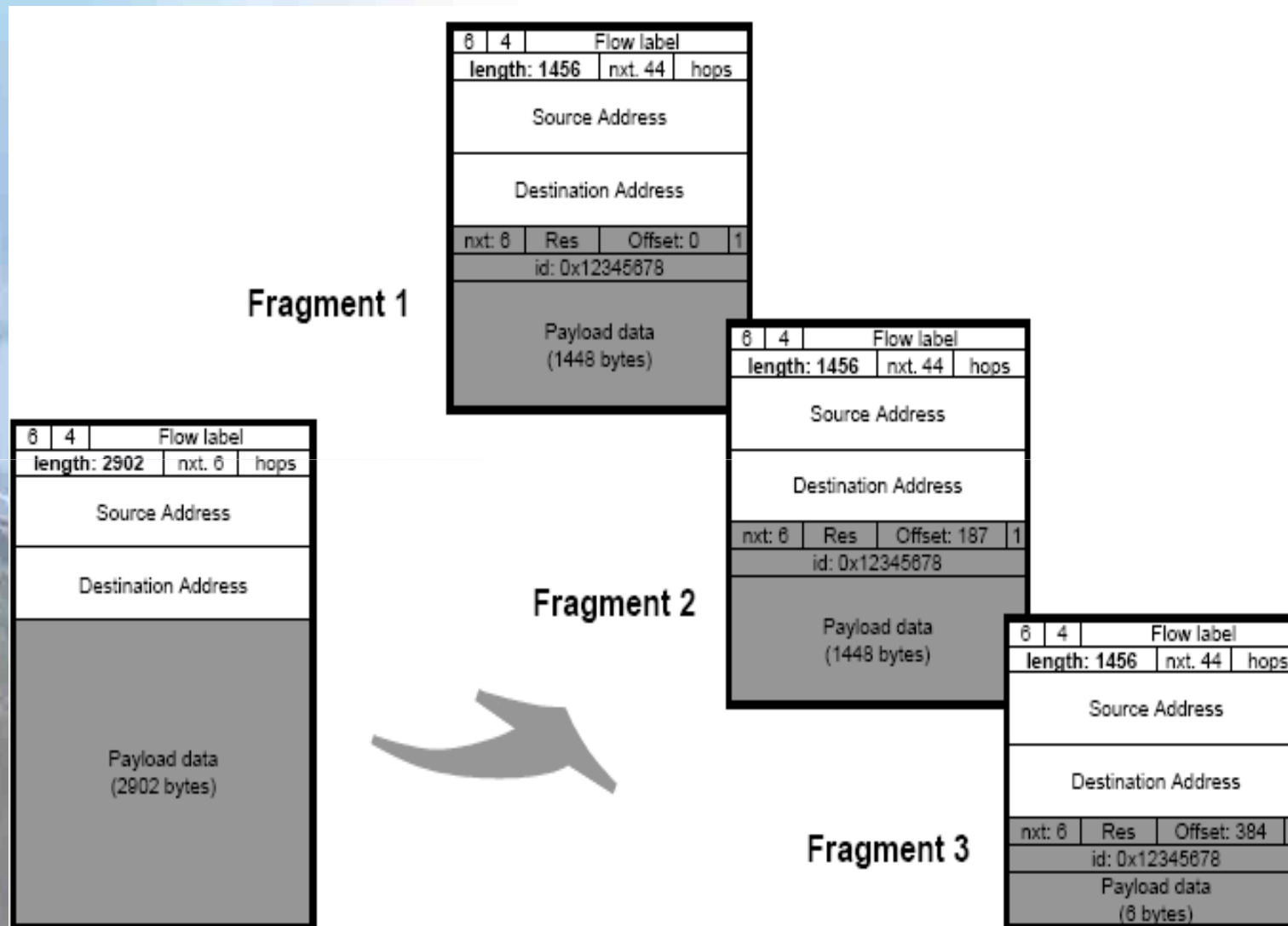
◆ Bit M

- il suo valore è posto a 1 in tutti i frammenti del datagramma tranne l'ultimo

◆ Fragment identification

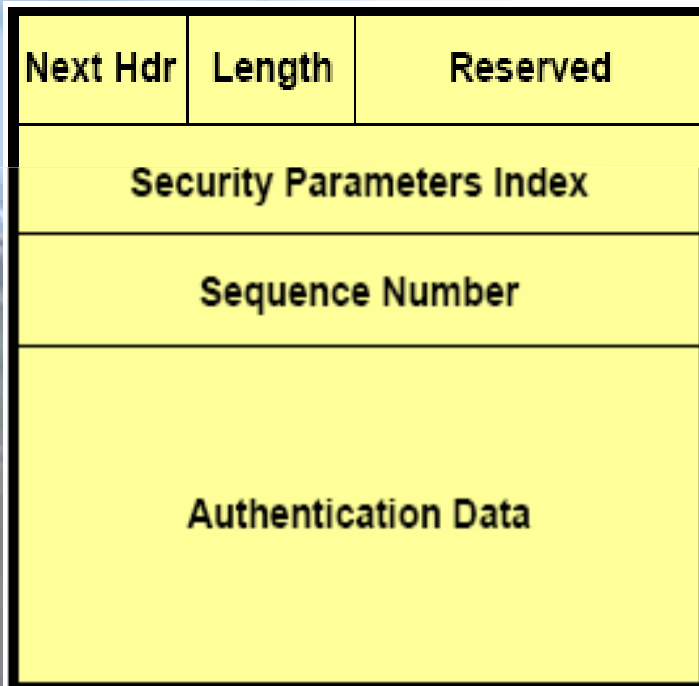
- identifica il datagramma a cui il frammento appartiene

Fragment Header 2/2



Authentication Header (AH)

- Assicura i servizi di verifica di integrità e di autenticazione dei pacchetti IP

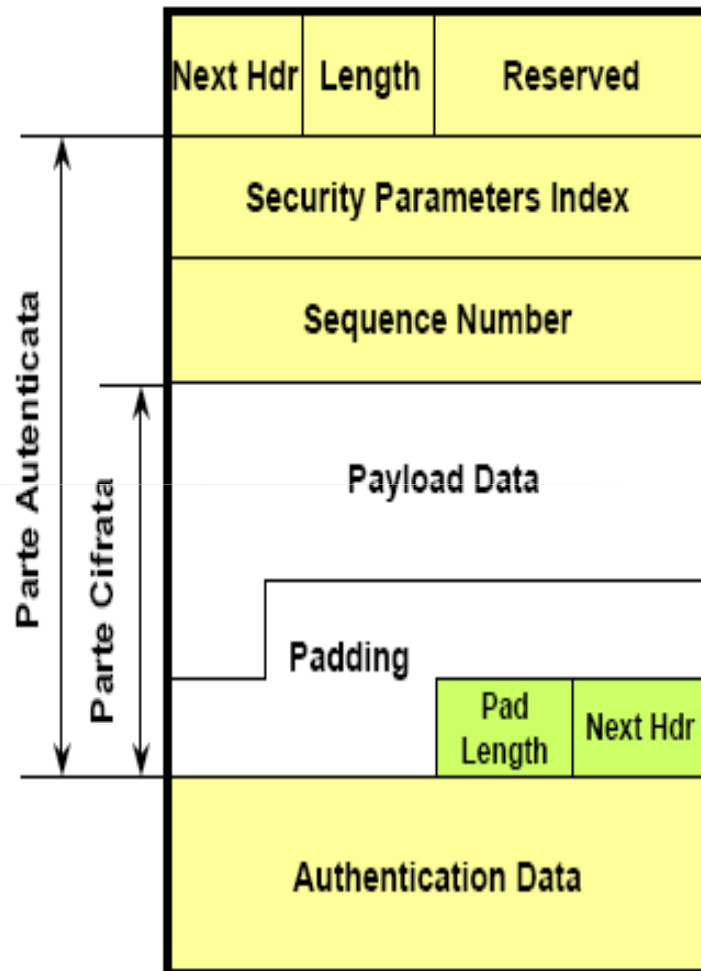


- Security Parameter Index(SPI) (32 bit)
 - ◆ definisce la Security Association
 - ◆ è usato in associazione con l'indirizzo di destinazione
- Sequence Number(32 bit)•
 - ◆ E' un numero monotonamente crescente
 - ◆ Nel primo pacchetto ha valore 1
 - ◆ È utilizzato per il servizio anti replay
- AuthenticationData (multiplo di 32 bit)
 - ◆ Il campo è calcolato mediante un qualsiasi algoritmo sulla base di
 - i bit del datagramma
 - la chiave segreta di cifratura
 - ◆ Il sistema IPSec ricevente verifica l'autenticità del datagramma compiendo la stessa operazione mediante la stessa chiave e confrontando i due risultati

Encapsulating Security Payload (ESP) 1/2

- Fornisce i servizi di
 - ◆ autenticazione e verifica di integrità dei pacchetti IP
 - ◆ Cifratura dei pacchetti IP
- I servizi di cifratura e di autenticazione possono essere attuati indipendentemente uno dall'altro
- Nel caso siano attivi entrambi i servizi, il ricevente eseguirà prioritariamente le funzioni di autenticazione, successivamente, in caso positivo le funzioni di decodifica
- Risparmio di processing e protezione verso attacchi del tipo denial of service

Encapsulating Security Payload (ESP) 2/2



- **Security Parameter Index(SPI) (32 bit)**
 - ◆ definisce la Security Association
 - ◆ è usato in associazione con l'indirizzo di destinazione
- **Sequence Number(32 bit)**
 - ◆ E' un numero monotonamente crescente
 - ◆ Nel primo pacchetto ha valore 1
 - ◆ È utilizzato per il servizio antireplay
- **Payload data**
 - ◆ Contiene i dati cifrati
 - Segmento TCP o UDP (Transportmode)
 - Pacchetto IP (Tunnel mode)
- **AuthenticationData**
 - ◆ Contiene l'ICV per l'autenticazione dei campi da SPI a Next header
 - ◆ È presente solo se è attivato il servizio di autenticazioneNext



IPv6 Indirizzamento

Indirizzamento IPv6

- **Dimensione 128 bit (16 bytes)**
 - ◆ Lo spazio equivale a circa 340.10^{12} indirizzi
 - ◆ Utilizzato con la stessa efficienza dello spazio degli indirizzi IPv4 consente di gestire 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

Formato degli indirizzi

- Nelle URL gli indirizzi tra parentesi quadre
 - ◆ `http://[2001:1:4F3A::206:AE14]:80/home.html`
 - ◆ ':' usato anche per separare No. porta da URL
- Necessario modificare Sw che usa URL
 - ◆ Browser ecc. Come in IPv4, indirizzi associati a interfacce di rete
- A ogni rete fisica e' assegnato un prefisso
- Possibile assegnare piu' prefissi alla stessa rete
- Possibile assegnare piu' indirizzi alla stessa interfaccia

Tipi di indirizzo

- Unicast: l'indirizzo specifica 1 interfaccia
 - ◆ Instradamento: percorso minimo
 - ◆ Un pacchetto che reca un indirizzo di questo tipo è consegnato esclusivamente a quella interfaccia
- Multicast: l'indirizzo specifica un gruppo di nodi
 - ◆ Identifica un insieme di interfacce
 - ◆ Un pacchetto che reca un indirizzo di questo tipo è consegnato a tutte le interfacce identificate dall'indirizzo
- Anycast: come il multicast ma
 - ◆ Identifica un insieme di interfacce
 - ◆ Pacchetto consegnato al nodo più vicino (in base alle metriche presenti sui router) al nodo mittente
- Broadcast eliminato
 - ◆ Pericoloso per attacchi DoS

Assegnazione degli indirizzi

- **0000 0000** - **compatibilita' IPv4**
- 0000 0001 - non assegnato
- **0000 001** - **indirizzi NSAP**
- **0000 010** - **Indirizzi IPX**
- 0000 011 - non assegnato
- 0000 1 - non assegnato
- 0001 - non assegnato
- **001** - **unicast globale di aggregazione**
- 010 - non assegnato
- 011 - non assegnato
- 100 - non assegnato
- 101 - non assegnato
- 110 - non assegnato
- 1110 - non assegnato
- 1111 0 - non assegnato
- 1111 10 - non assegnato
- 1111 110 - non assegnato
- 1111 1110 0 - non assegnato
- **1111 1110 10** - **indirizzi unicast locali di collegamento**
- **1111 1110 11** - **indirizzi unicast locali del sito**
- **1111 1111** - **indirizzi multicast**

Spazio degli indirizzi

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

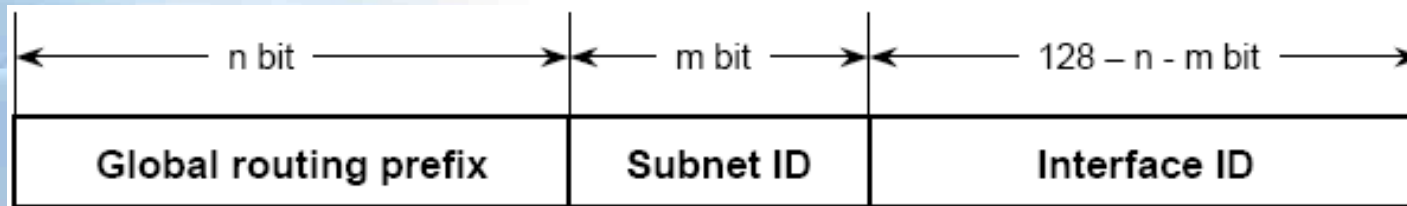
Tipo di indirizzo	Prefisso (binario)	Notazione IPv6
Non specificato	000....0 (128 bit)	::/128
Loopback	000....1 (128 bit)	::1/128
Multicast	11111111	FF00::/8
Link-local Unicast	1111111010	FE80::/10
Site-local Unicast	1111111011	FECO::/10
Global Unicast	Qualsiasi altro	

Indirizzi unicast

- Unspecified
- Loopback
- IPv4 Compatible
- IPv4 Mapped
- Indirizzi Scoped
 - ◆ Unicast locale di collegamento
 - ◆ Unicast locale di sito
 - ◆ Unicast globale di aggregazione

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 Global

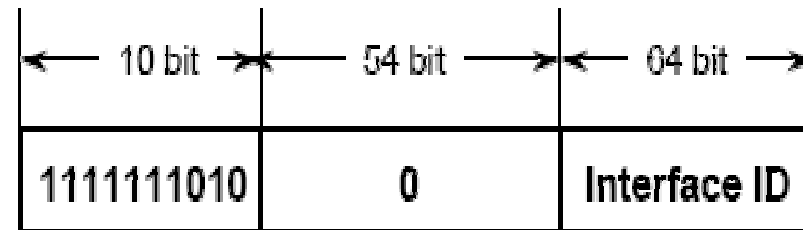
Indirizzi Speciali Unicast 1/2

- 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
 - ◆ Identifica l'interfaccia stessa
 - ◆ Analogo a 127.0.0.1 IPv4 (localhost)
 - ◆ ping6 ::1 -> verifica il funzionamento dello stack IPv6

Indirizzi Speciali Unicast 2/2

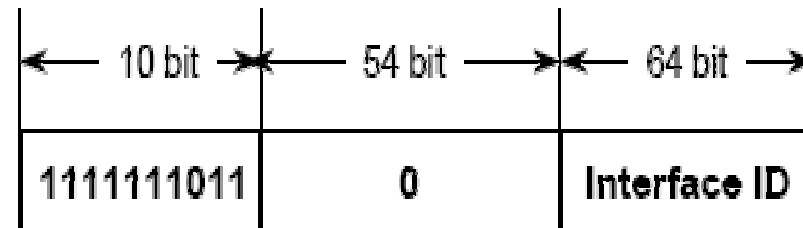
- Indirizzi Link-local

- ◆ 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



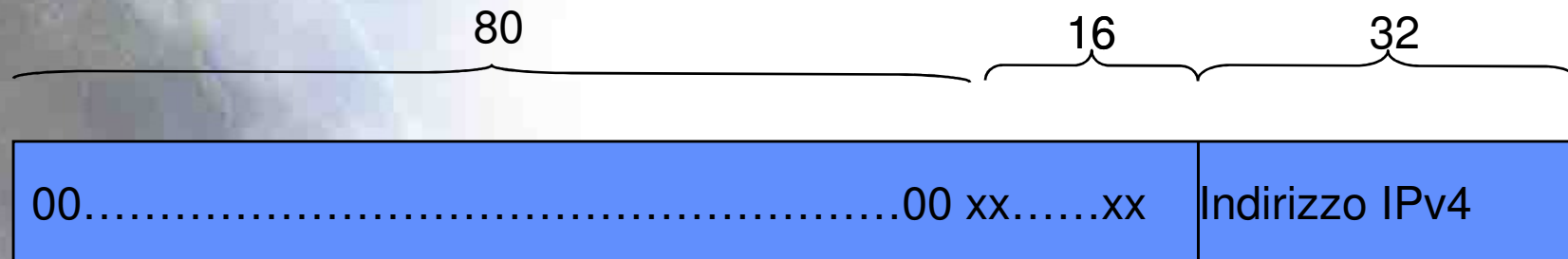
- Indirizzi Site-local

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



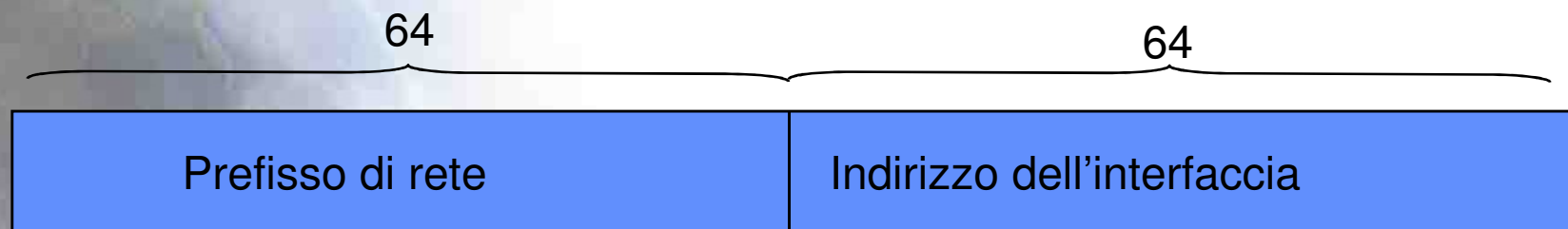
Indirizzi incorporati IPv4

- Usano una parte dello spazio riservato
 - ◆ Prefisso 0000 0000
- Primi 80 bit a 0
- 16 bit seguenti a 0:0:0:0 o F:F:F:F
 - ◆ 0:0:0:0 -> IPv4 compatible
 - ◆ F:F:F:F -> IPv4 mapped
- Restanti 32 bit contengono indirizzo IPv4
- Usati nella transizione IPv4 -> IPv6



Indirizzi unicast scoped - formato

- Indirizzi unicast consistono di due parti
- L'indirizzo di interfaccia puo' essere assegnato
 - ◆ Manualmente
 - ◆ Usando direttamente l'indirizzo MAC
 - Potenziali vantaggi in efficienza
 - Interoperabilita' con i protocolli MAC esistenti

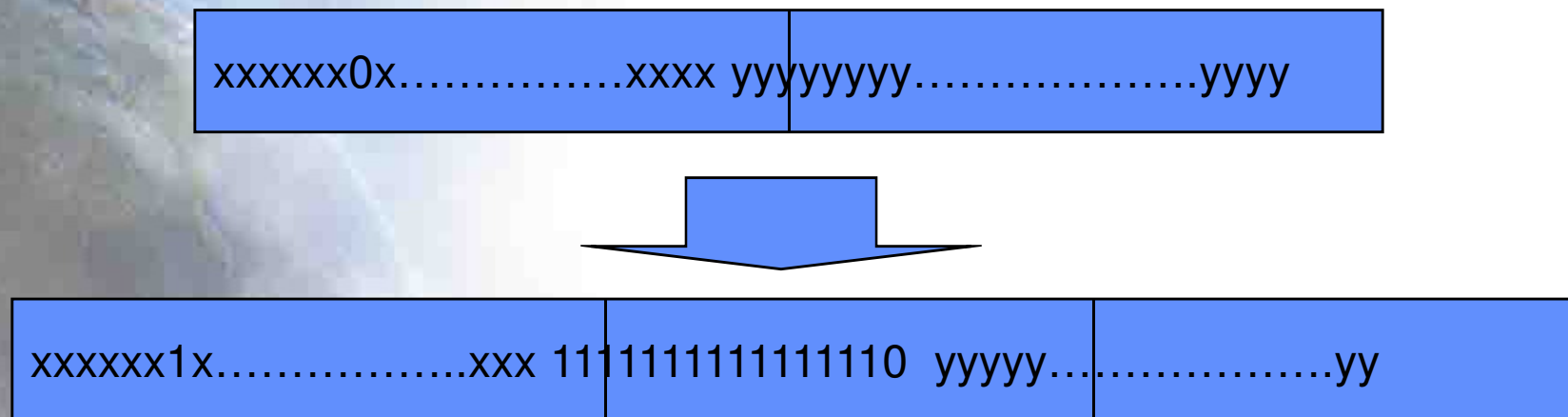


Indirizzo di interfaccia

- Dipende dal formato dell'indirizzo fisico dell'interfaccia
- Codifica EUI64
 - ◆ Codifica IEEE che estende a 64 bit la codifica EUI48 (standard Ethernet)
- Se la codifica dell'indirizzo fisico e' EUI64 l'indirizzo di interfaccia si ottiene in modo diretto
- Altrimenti servono soluzioni ad hoc


Indirizzo MAC -> ID interfaccia

- Si inserisce la sequenza FFFE dopo i primi 24 bit
- Esempio
 - ◆ Indirizzo Ethernet: 00-AA-00-3F-2A-1C
 - ◆ Indirizzo EUI64: 00-AA-00-FF-FE-3F-2A-1C
 - ◆ Indirizzo IPv6: 02:AA:00:FF:FE:3F:2A:1C
 - Il settimo bit viene posto ad 1 (nell'indirizzo EUI64 e' sempre 0)



Privacy

- Indirizzo fisico associato a un dispositivo
 - ◆ Piu' facilmente associabile a una persona
- Il prefisso di rete puo' cambiare
- L'indirizzo IPv6 dell'interfaccia rimane lo stesso se viene ricavato da quello fisico
- RFC 3041: generare l'identificatore di interfaccia in modo casuale



Transazione da IPv4 a IPv6

Scenario

- IPv4 e IPv6 incompatibili
 - ◆ Stesso strato OSI
 - ◆ Svolgono le stesse funzioni
- Requisiti per IPv6
 - ◆ Garantire la compatibilit  con i dispositivi esistenti
 - ◆ Offrire meccanismi semplici per la transizione IPv4 -> IPv6
- Evoluzione graduale
 - ◆ Non vi sar  una transizione brusca
 - ◆ I due protocolli conviveranno per alcuni anni
- I meccanismi di transizione sono stati al centro dell'attenzione nella progettazione di IPv6

Evoluzione in tre fasi

- Prima fase
 - ◆ Si usa principalmente l'infrastruttura IPv4 esistente
- Seconda fase
 - ◆ I protocolli coesistono
- Terza fase
 - ◆ I nodi IPv4 restanti usano l'infrastruttura IPv6
 - ◆ Essi devono poter usare i servizi IPv6

Meccanismi di transizione

I meccanismi di transizione possono essere suddivisi in tre categorie fondamentali:

- Implementati sugli host
 - ◆ Es. host dual stack
 - ◆ Altri: BIS, BIA, ...
- Implementati a livello di rete
 - ◆ Es. tunnel
 - Manuali, 6to4, automatici
 - ◆ Rete Dual Stack
- Basati su traduttori di protocollo
 - ◆ Es. SIIT, NAT-PT

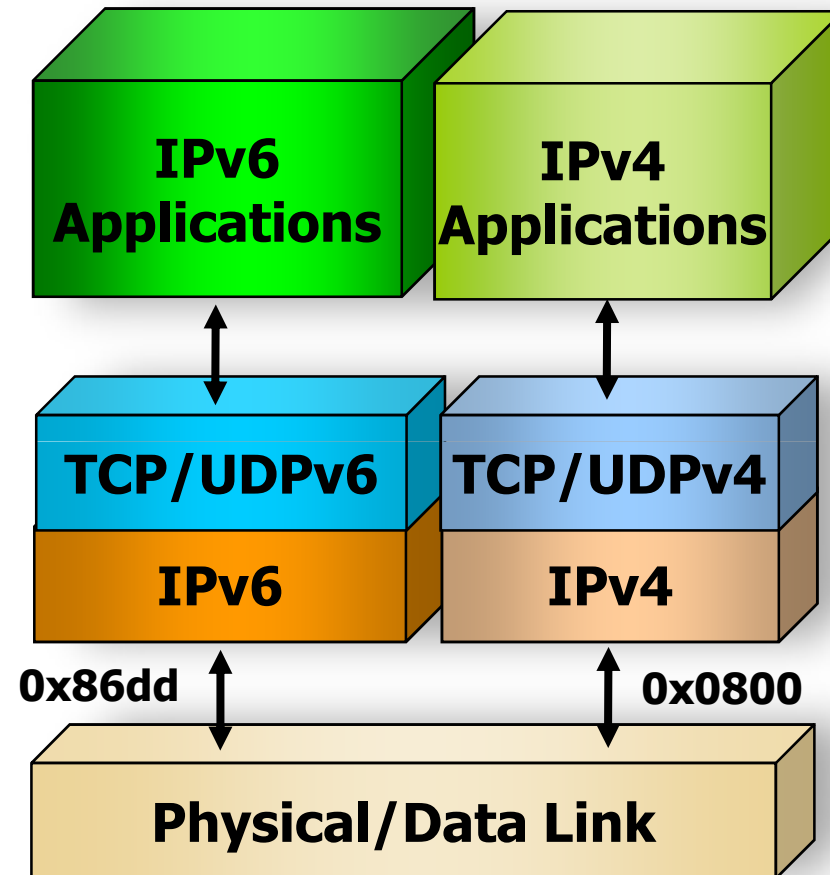


Transazione da IPv4 a IPv6

Implementazione su host

Host dual stack

- Nodo dual stack
 - ◆ Implementa entrambi i protocolli
 - ◆ Assegna indirizzi IPv4 e IPv6 alla stessa interfaccia
- Le applicazioni che usano IPv4 usano i servizi dello strato corrispondente
- È il modo più diretto per mantenere la compatibilità tra due sezioni di rete utilizzando le due versioni del protocollo Ethernet IPv4 TCP Appl.



Vantaggi/svantaggi

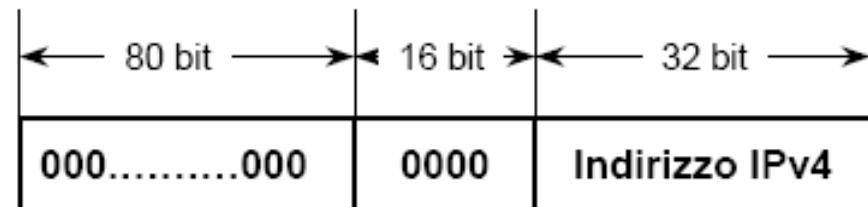
- Vantaggi:
 - ◆ Schema semplice
 - ◆ Non richiede alcun supporto particolare
- Svantaggi
 - ◆ Richiede la gestione di una doppia infrastruttura di rete
 - ◆ Non fa nulla per integrare IPv4 e IPv6
 - Dal punto di vista di un nodo dual stack le due reti sono completamente separate
 - E' un meccanismo di compatibilità più che di transizione
- Soluzione attualmente più usata

Indirizzi IPv4 immersi

- Sono previste due modalità

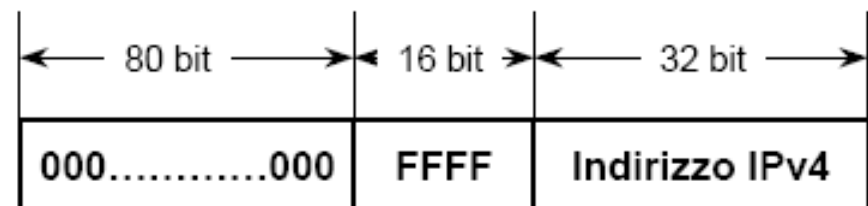
- IPv4-compatible address

- ◆ Sono utilizzati quando è necessario effettuare tunnel di pacchetti IPv6 attraverso reti IPv4



- IPv4-mapped IPv6 address

- ◆ Sono utilizzati da host IPv6 per indirizzare host che supportano solo il protocollo IPv4





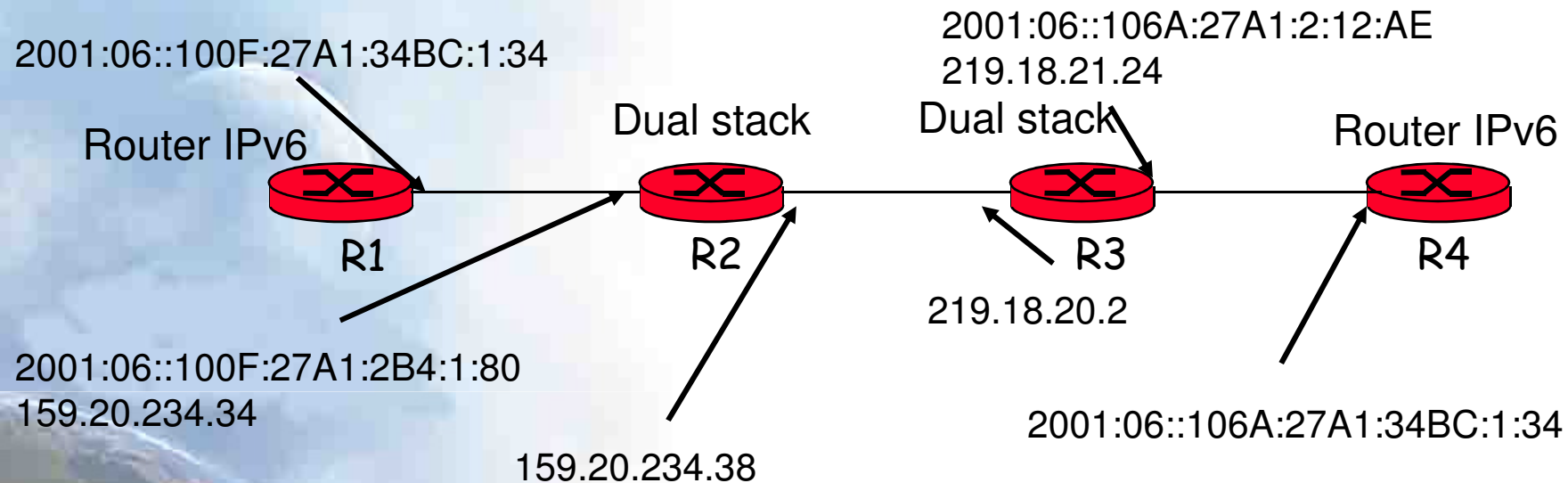
Transazione da IPv4 a IPv6

Implementazione a livello rete

Tunnel IPv6-IPv4

- Tunnel: usati normalmente per trasportare pacchetti di un protocollo in una rete basata su un protocollo diverso
- I tunnel IPv6-in-IPv4 permettono di utilizzare IPv6 senza disporre di una infrastruttura di rete IPv6 nativa
- IPv6-in-IPv4
 - ◆ Permettono a pacchetti IPv6 di attraversare una rete IPv4
 - ◆ Pacchetto IPv6 incapsulato in un pacchetto IPv4

Tunnel IPv6-IPv4 - esempio

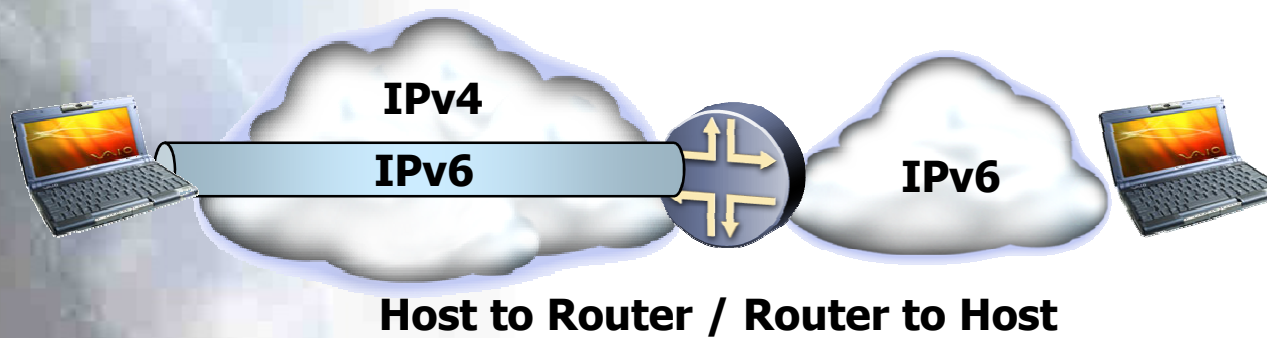
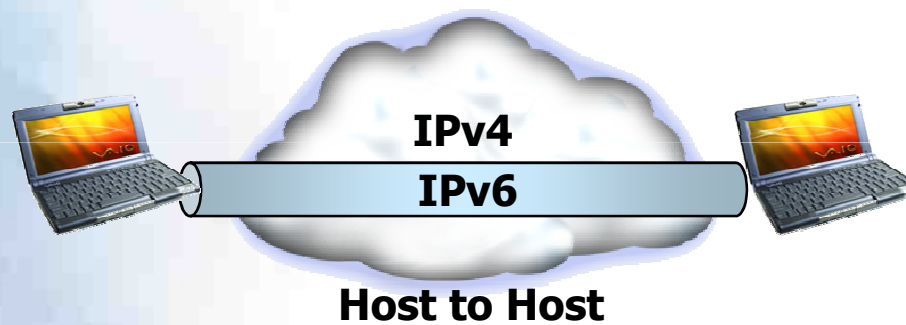
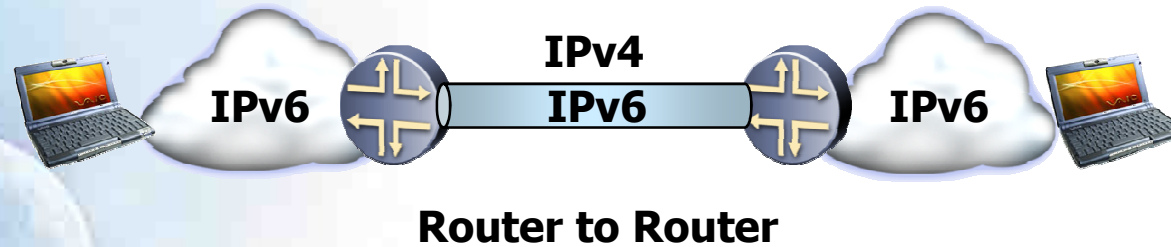


- R2
 - ◆ Incapsula pacchetto proveniente da R1
 - ◆ Spedisce pacchetto IPv4 risultante a R3
 - Indirizzo destinazione 219.18.20.2
- R3
 - ◆ Estrae pacchetto IPv6 da pacchetto IPv4 ricevuto da R2
 - ◆ Invia pacchetto IPv6 a R4

Tunnel IPv6-IPv4

- I punti di ingresso e uscita dai segmenti IPv4 devono essere nodi dual stack
- Da fuori, il tunnel appare come un solo hop IPv6
 - ◆ Dal punto di vista IPv6 è come se la rete IPv4 fosse semplicemente una tecnologia trasmissiva di livello due
- MTU (Maximum Transfer Unit)
 - ◆ Più piccola di 20 byte
 - A causa della presenza dell'header IPv4
- Topologie possibili:
 - ◆ Router verso router
 - ◆ Host verso router
 - ◆ Host verso host

Esempi di Tunnel



Configurazione dei tunnel

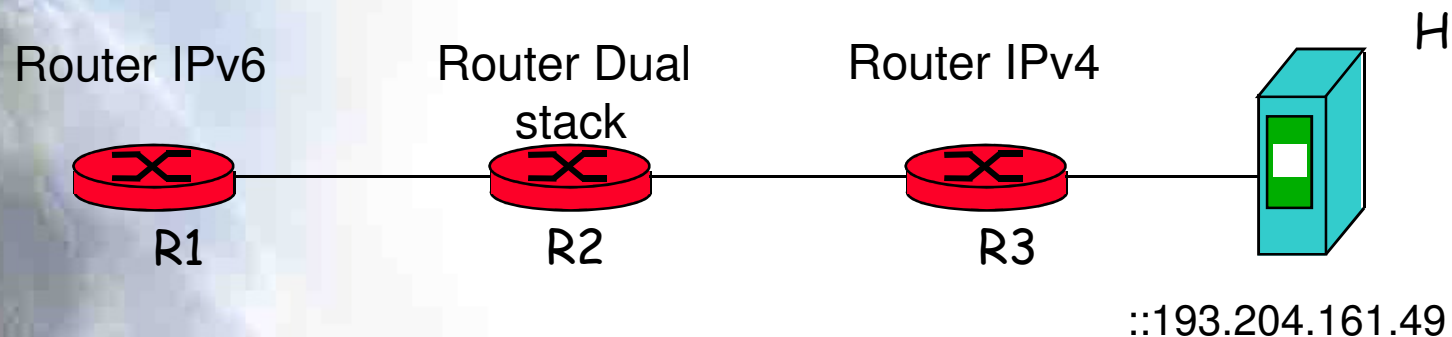
- Tunnel manuali
 - ◆ Sono configurati manualmente agli estremi (R2 ed R3 nell'esempio)
 - ◆ Usati per creare tunnel permanenti tra due estremi
 - ◆ Ampiamente usati
- Tunnel broker
 - ◆ Applicazione Web raggiungibile via IPv4
 - ◆ Crea dinamicamente un tunnel su richiesta
 - ◆ Adatto per utenti occasionali

Altri tipi di tunnel

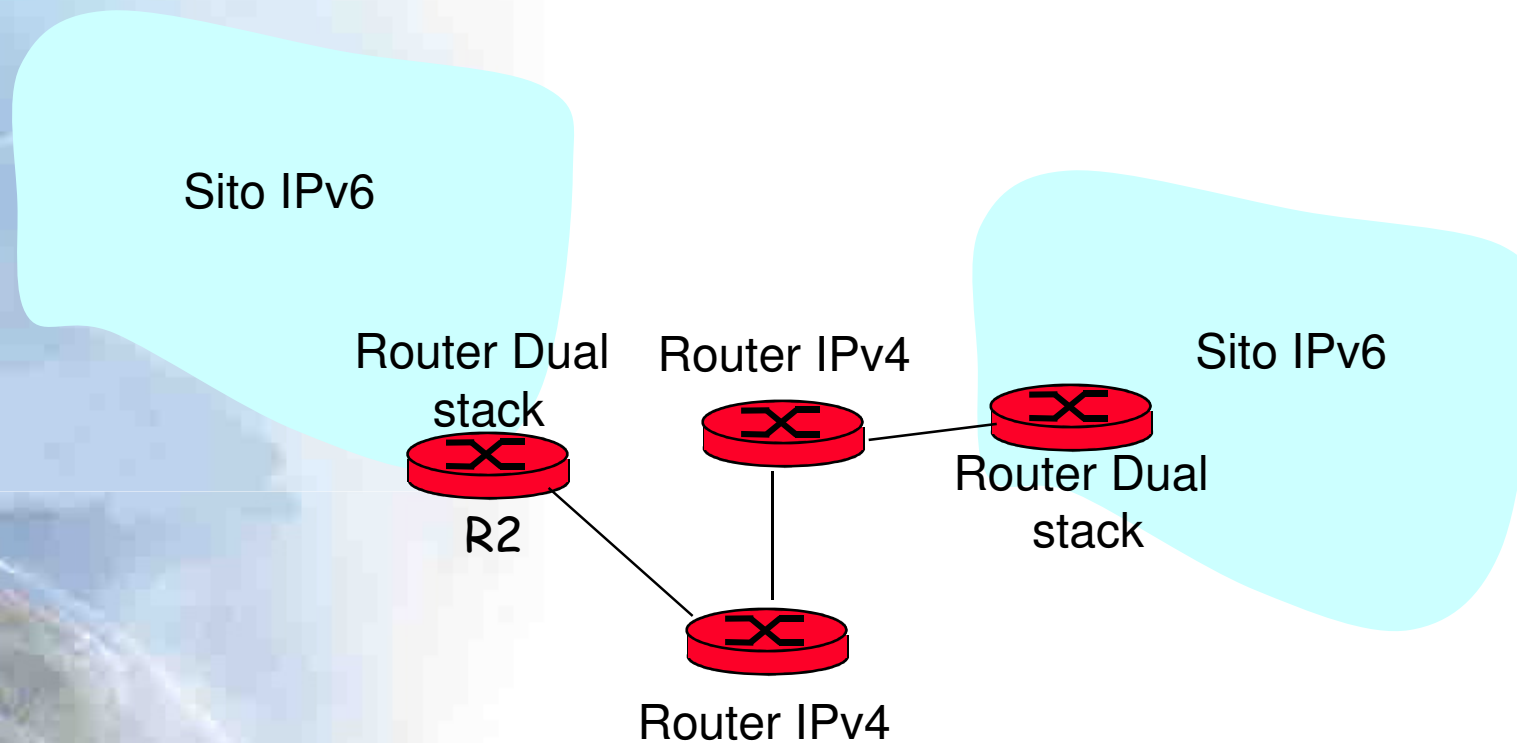
- Tunnel automatici
 - ◆ Indirizzi IPv4 degli estremi del tunnel ottenuti automaticamente
 - ◆ Usano gli indirizzi IPv4 compatibile
- Tunnel 6-to-4
 - ◆ Permettono di connettere tra loro siti IPv6 usando un indirizzo IPv4 pubblico per ogni sito

Tunnel automatici - Esempio

- Pacchetto IPv6 diretto da R1 a H
- Indirizzo H IPv4-compatibile
- Indirizzo IPv4 di H si ottiene automaticamente da quello IPv6
- Estremo (H) deve coincidere con il destinatario del messaggio



Tunnel 6to4



- La rete IPv6 deve avere il prefisso 2002::/16 (assegnato dalla IANA)

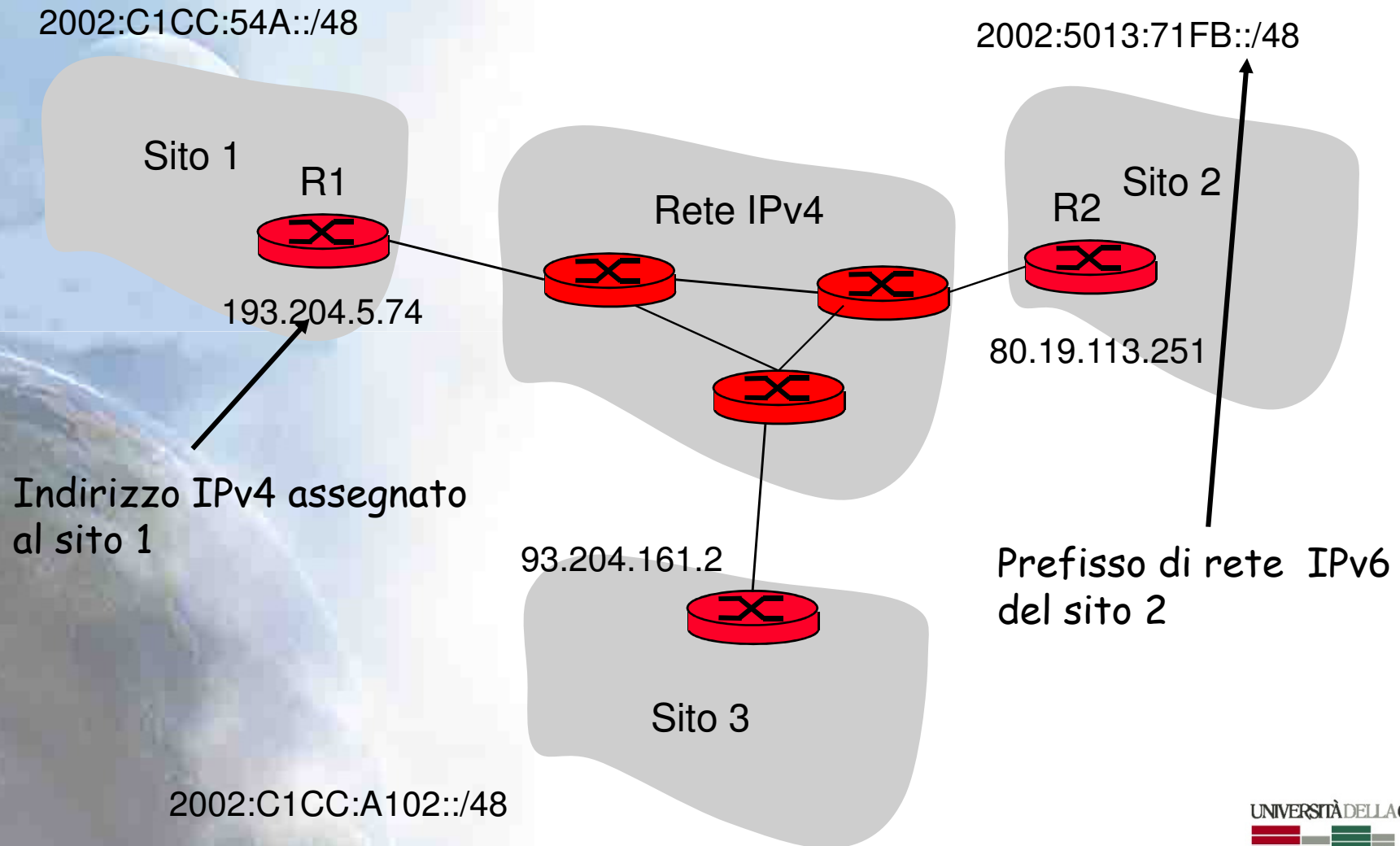
Tunnel 6to4 - formato indirizzo

- Ogni sito IPv6 che usa il tunnel riceve un indirizzo IPv4 unico
 - ◆ Corrisponde al router dual stack di bordo
- Formato di un pacchetto che usa un tunnel 6to4
2002:<indirizzo IPv4 sito dest.><indirizzo di sottorete><indirizzo di interfaccia>

Tunnel 6to4: funzionamento

- Un pacchetto destinato a un indirizzo 6to4:
 - ◆ Viene instradato fino ad un router 6to4
 - È un router configurato per instradare la rete 2002::/16 su 6to4
 - Normalmente è il router di bordo di un'organizzazione (o site)
 - ◆ Per inoltrarlo, il router
 - Esamina l'indirizzo destinazione e deduce l'estremo del tunnel
 - Incapsula il pacchetto e lo inoltra sulla rete IPv4
 - ◆ All'altro estremo del tunnel il pacchetto viene decapsulato ed instradato normalmente nel site

Tunnel 6to4 – esempio 1/2



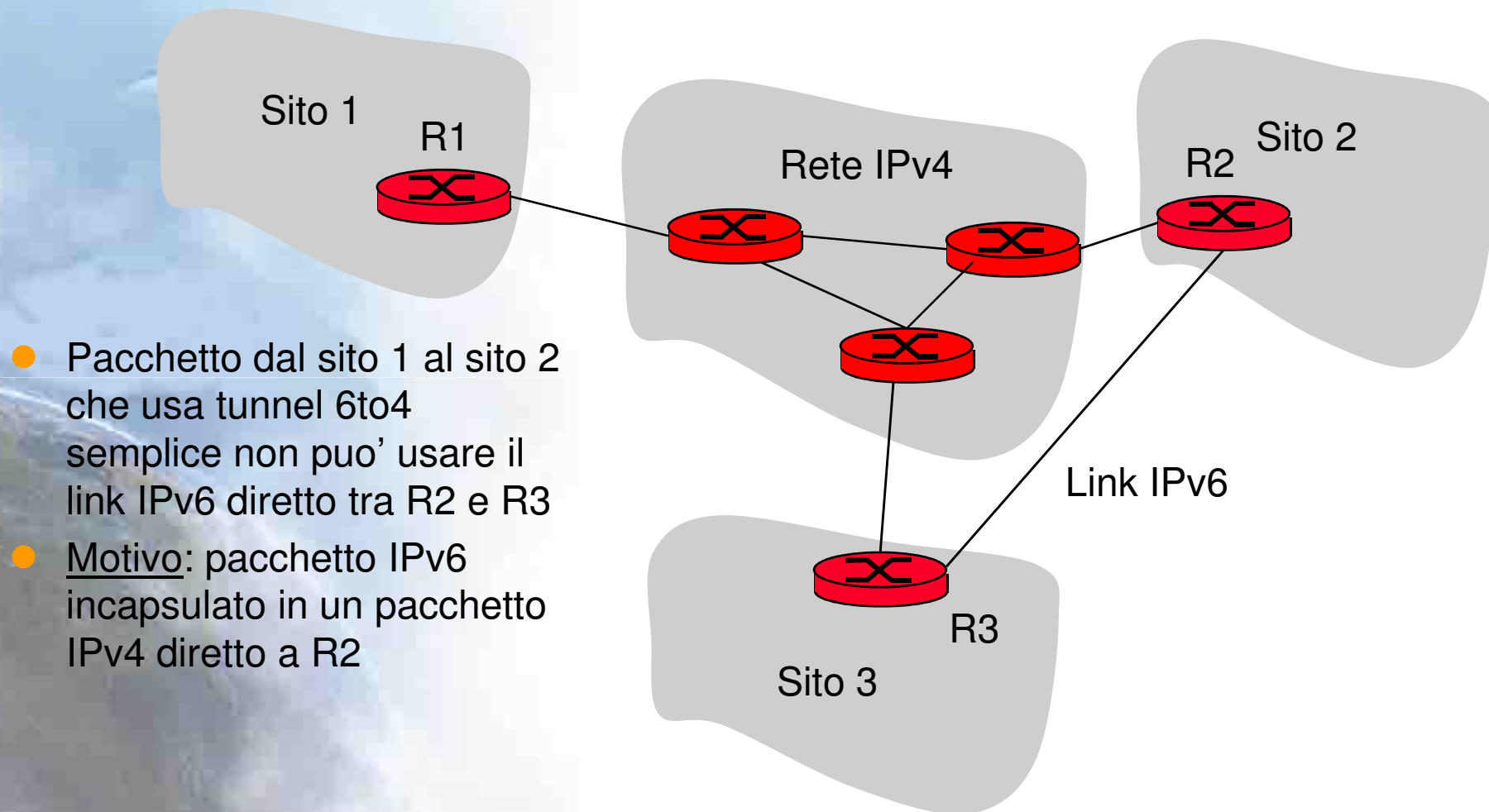
Tunnel 6to4 – esempio 2/2

- Pacchetto dal sito 1 al sito 2
- Pacchetto IPv6 raggiunge router di bordo dual stack R1
 - ◆ R1 deduce l'indirizzo IPv4 di R2 da indirizzo IPv6 della destinazione
 - ◆ R1 incapsula pacchetto IPv6 in pacchetto IPv4 con destinazione 80.19.113.251
- R2 riceve pacchetto
 - ◆ Estrae pacchetto IPv6
 - ◆ Consegna pacchetto IPv6 alla destinazione nel sito 2

Vantaggi/svantaggi

- Semplice da implementare
- Non sfrutta eventuali segmenti IPv6 attraversati

Esempio

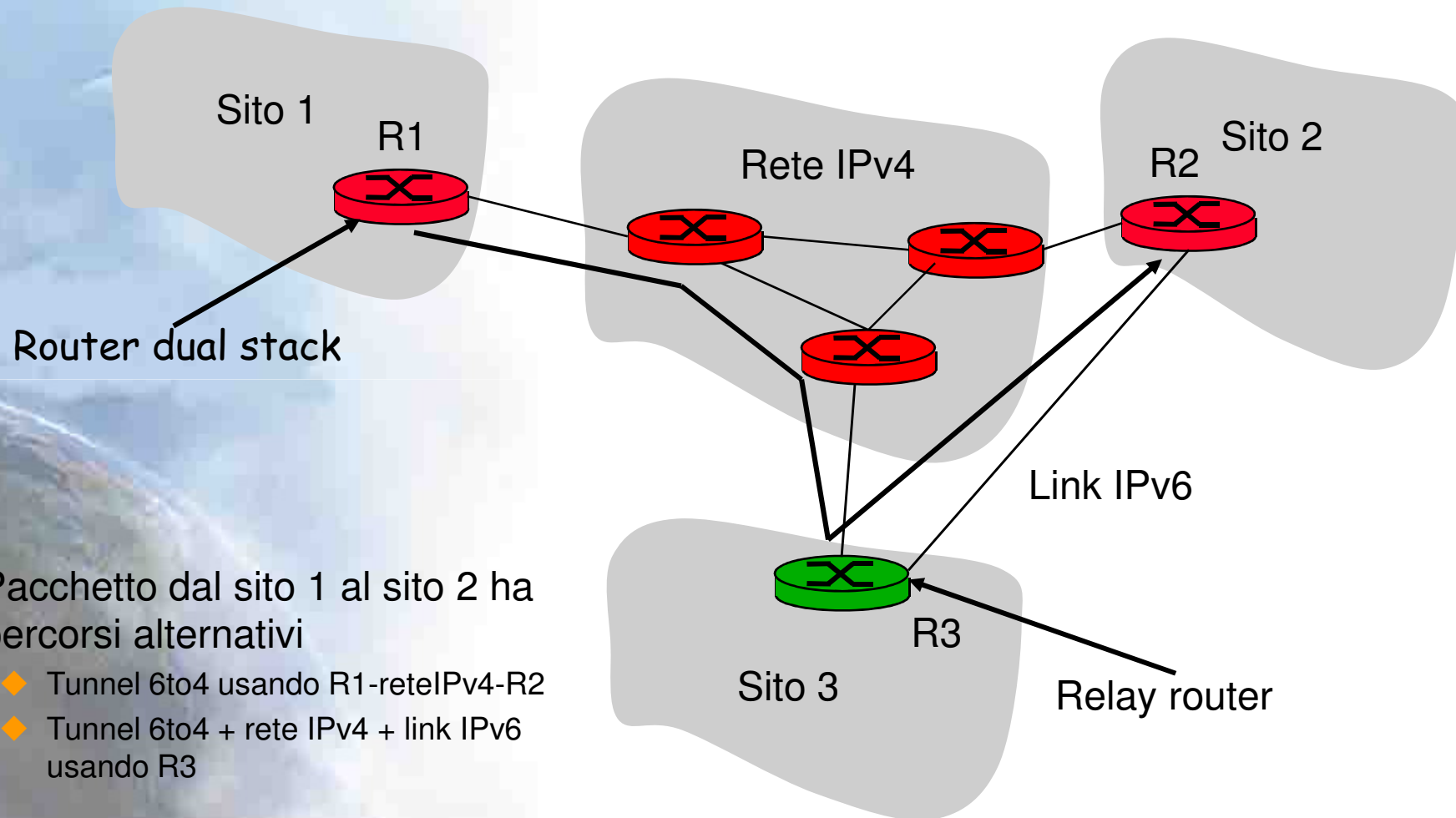


- Pacchetto dal sito 1 al sito 2 che usa tunnel 6to4 semplice non può usare il link IPv6 diretto tra R2 e R3
- Motivo: pacchetto IPv6 incapsulato in un pacchetto IPv4 diretto a R2

6to4 Relay router

- In questa forma 6to4 permette la comunicazione tra site che utilizzano indirizzi 6to4, ma non permette la comunicazione con il resto della rete IPv6:
 - ◆ Nodi sulla rete IPv6 possono inviare pacchetti verso destinazioni 6to4 tramite un router 6to4
- Soluzione:
 - ◆ Relay router: router disposto a offrire accesso alla rete IPv6 a pacchetti tunnel 6to4
 - ◆ Impiega la banda di chi lo mette a disposizione
 - ◆ Indirizzo anycast per i relay router: 2002:C058:6301::
 - ◆ Indirizzo IPv4 corrispondente: 192.88.99.1
 - ◆ Esistono relay router pubblici

6to4 Relay router - esempio



- Pacchetto dal sito 1 al sito 2 ha percorsi alternativi
 - ◆ Tunnel 6to4 usando R1-retelIPv4-R2
 - ◆ Tunnel 6to4 + rete IPv4 + link IPv6 usando R3

6to4 - vantaggi e svantaggi

- Vantaggi

- ◆ Semplice da configurare
- ◆ Permette di usare IPv6 senza disporre di indirizzi e senza avere un provider IPv6 nativo

- Svantaggi

- ◆ Indirizzi IPv6 di un sito legati all'indirizzo IPv4 del router di bordo
 - Se cambia indirizzo IPv4 di sito il sito va rinumerato
- ◆ I relay router possono essere lontani
 - Sia dalla sorgente che dalla destinazione

Sommario

- Tunnel configurati
 - ◆ Necessario configurare manualmente gli estremi
 - ◆ Comuni
- Tunnel automatici
 - ◆ Basati sugli indirizzi IPv4-compatibili
 - ◆ Deprecati
- Tunnel 6to4
 - ◆ Instradamento manuale
 - ◆ Selezione automatica dell'estremo