



## Introduzione a IP versione 6

**Davide Quaglia**  
a.a. 2008/2009

1

## Requisiti

- Miliardi di indirizzi per evitare esaurimento anche in caso di assegnamento non ottimale
- Riduzione della dimensione delle tabelle di routing
- Semplificazione per consentire ai router di elaborare i pacchetti ancora più velocemente
- Migliore sicurezza (autenticazione e riservatezza)
- Migliore supporto per applicazioni in tempo reale (ad es. multimediali)
- Miglioramento del multicast
- Possibilità di host mobili senza cambiare indirizzo
- Possibilità di modificare il protocollo in futuro
- Coesistenza tra vecchio TCP/IP e IPv6

4

## Sommario

- Introduzione
  - Motivazione e cronologia
  - Requisiti
  - Coesistenza tra IPv6 e IPv4
- Formato del pacchetto
- Indirizzamento
- Autoconfigurazione
- Capacità di instradamento avanzate
- Bibliografia

2

## Coesistenza tra vecchio TCP/IP e IPv6

- IPv6 non è compatibile con IPv4
- IPv6 è compatibile con i protocolli che “stanno sopra” al protocollo IP
  - Protocolli di Trasporto: TCP, UDP
  - Protocolli di segnalazione: ICMP, IGMP
  - Protocolli di routing: OSPF, BGP
  - Protocolli applicativi: DNS, HTTP, ecc...

5

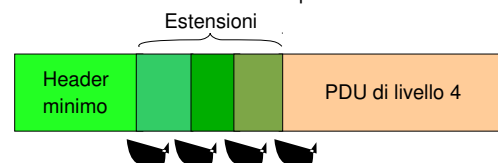
## Motivazione e Cronologia

- Esaurimento degli indirizzi
  - A causa dell'assegnazione a classi
- Requisiti diversi per utenti diversi
  - Utenza residenziale
  - Utenza mobile
  - Necessità di garanzie di QoS per certe applicazioni
  - Reti di sensori (→ Internet of Things)
- Nel 1990 Internet Engineering Task Force (IETF) iniziò a lavorare su una nuova versione di IP
  - RFC 1550 apre la discussione
- Nel 1993 prende forma IPv6

3

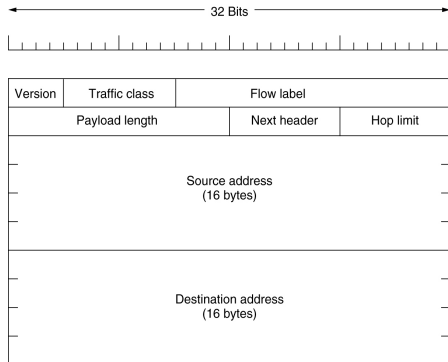
## Dimensione dell'header IP

- Nella maggior parte dei pacchetti, certi campi del vecchio IPv4 non erano usati
- Occorre da un lato ridurre gli sprechi, dall'altro introdurre un modo efficiente per gestire le informazioni solo quando servono
  - Header minimo + estensioni opzionali



6

## Header minimo del pacchetto IPv6



7

## Estensioni dell'header

- Se presenti devono apparire nell'ordine della tabella
- Lunghezza variabile (ma almeno 8 byte)
- Campi opzionali sono specificati nel formato `type|length|value`

Extension header	Description
Hop-by-hop options	Miscellaneous information for routers
Destination options	Additional information for the destination
Routing	Loose list of routers to visit
Fragmentation	Management of datagram fragments
Authentication	Verification of the sender's identity
Encrypted security payload	Information about the encrypted contents

10

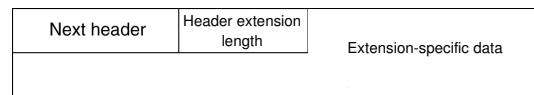
## Header minimo del pacchetto IPv6

- Version (4 bit): ha valore 6
- Traffic class (8 bit): eredita le funzioni del ToS
- Flow label (20 bit): assieme a Src Addr e Dest Addr può servire a creare una label per funzioni "tipo MPLS"
- Payload length (16 bit): lunghezza del payload
- Next header (8 bit): codice della prossima intestazione o del tipo di PDU di livello 4
- Hop limit (8 bit): eredita le funzioni del TTL
- Source address (128 bit): vedere slide sul formato
- Destination address (128 bit): vedere slide sul formato

8

## Formato delle estensioni

- Next header (1 byte): indica l'intestazione che segue oppure la PDU di livello 4
- Header extension length (1 byte): lunghezza dell'estensione – 8 (8 byte è la dim minima)



11

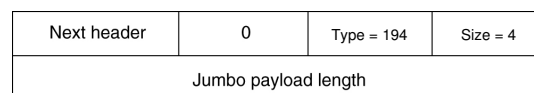
## Differenze rispetto a header IPv4

- L'header ha lunghezza fissa (40 byte)
- Eliminazione campo *IP Header Length*
- Eliminazione campo *Protocol* (esiste *next header*)
- Eliminazione dei campi per gestire la frammentazione
  - E' stata ridotta la necessità di frammentare (minore lavoro nei router → maggiore throughput)
  - E' stata introdotta un'estensione di header quando serve
- Eliminazione del campo *Checksum* che doveva essere ricalcolata in ogni router
  - minore lavoro nei router → maggiore throughput

9

## Esempio di hop-by-hop options: opzione per grandi pacchetti

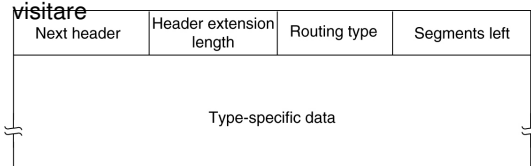
- Usato per indicare lunghezze maggiori di 64KB
- Type (1 byte): 194 = opzione per grandi pacchetti
- Size (1 byte): 4 = "la dimensione è su 4 byte"
- Jumbo payload length (4 byte): dimensione (valore > 65536)
- Grandi pacchetti aumentano l'efficienza di reti veloci perché ammortizzano il tempo fisso di elaborazione



12

## Esempio di estensione per il routing

- Routing type (1 byte): per ora è stato definito solo il codice 0 = source routing
- Type-specific data: in caso di source routing sono elencati una serie di indirizzi IPv6 di router attraverso cui passare
- Segments left (1 byte): nr. di router ancora da visitare



13

## Formato degli indirizzi

- 128 bit (16 byte)
- Notazione: 8 gruppi (separati da ":") di 4 cifre esadecimali
  - 8000:0000:0000:0000:0023:0567:0000:CDEF
- Abbreviazioni:
  - Si possono omettere gli zeri iniziali di un gruppo
    - 8000:0000:0000:0000:23:567:0:CDEF
  - Gruppi contenenti solo zeri possono essere sostituiti da una coppia di ":" (vale per UNA SOLA sequenza di gruppi a zero)
    - 8000::123:4567:0:CDEF

16

## Frammentazione

- Solo l'host mittente può frammentare i pacchetti (in IPv4 anche i router potevano frammentare)
  - Il lavoro dei router viene semplificato aumentandone il throughput
  - Se un router riceve un pacchetto troppo grande lo scarta e manda all'host mittente un messaggio ICMP
- I campi relativi alla frammentazione sono contenuti in una estensione opzionale dell'header
- Header minimo e eventuali header opzionali non possono essere frammentati

14

## Formato degli indirizzi (2)

- Gli indirizzi IPv4 possono essere scritti in due modi:
  - Padding con (128-32) bit a "0"
    - notazione IPv6
    - in notazione decimale puntata (o "dotted") portata a 128 bit con degli zeri (rappresentati da una coppia di ":")
      - ::157.27.242.10
  - Antependendo 16 bit a "1" ai 32 bit dell'indirizzo e i restanti (128-16-32) messi a "0"
    - Notazione IPv6
    - in notazione decimale puntata portata a 128 bit con il prefisso "::FFFF:"
      - ::FFFF:157.27.242.10

17

## Estensioni dell'header per la sicurezza

- L'estensione *Authentication* serve per determinare con sicurezza l'identità del mittente
- L'estensione *Encrypted Security Payload* serve per cifrare il payload in modo da proteggerne il contenuto da occhi indiscreti
- Entrambe queste estensioni derivano da ciò che in IPv4 si chiamava *IPSec*

15

## Tipi di indirizzi

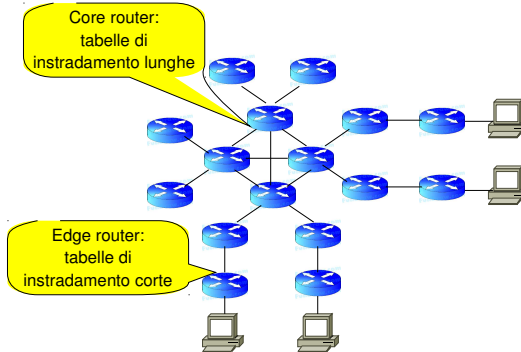
- Non esistono più le classi
- Indirizzo non assegnato: 00..0 (tutti 128 bit a 0)
- Indirizzo di loopback: 00..1 (127 zeri e un "1")
- Multicast: FFxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx
- Indirizzi privati
  - Link local unicast: iniziano con i bit 1111 1110 10
    - da usare nella procedura di *autoconfigurazione* (vedi lucido apposito)
  - Site local unicast: iniziano con i bit 1111 1110 11
    - da usare in intranet (indirizzi privati mai propagati su Internet)
- Unicast global addresses
  - indirizzi pubblici
  - attualmente sono assegnati quelli che iniziano con i bit 001<sub>18</sub>

## Netmask

- La maschera di bit indicava quale parte dell'indirizzo era da considerarsi come prefisso della rete
  - Es: 157.27.242.10/255.255.255.0
- Negli ultimi anni si era affermata la notazione "/XX"
  - Es: 157.27.242.10/24
- In IPv6 rimane solo quest'ultima notazione
  - Es: 8000:0000:0000:0000:0123:4567:89AB:CDEF/112

19

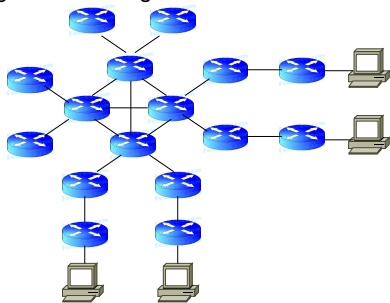
## Problema dell'assegnamento degli indirizzi (3)



22

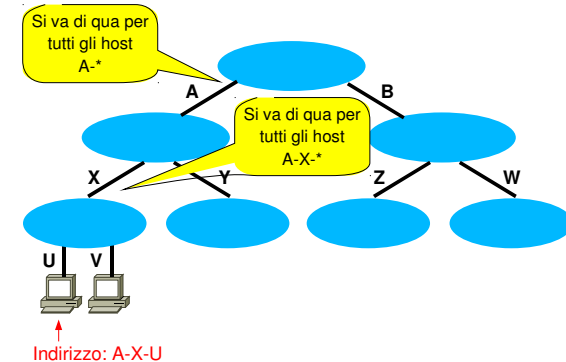
## Problema dell'assegnamento degli indirizzi

- La rete Internet, come anche la rete telefonica, ha una organizzazione gerarchica



20

## Indirizzi gerarchici



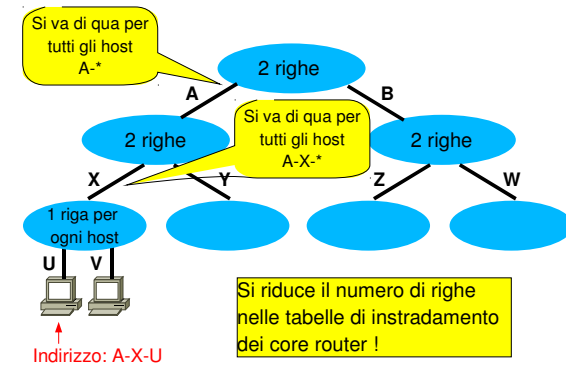
23

## Problema dell'assegnamento degli indirizzi (2)

- I numeri del telefono riflettono la gerarchia della rete telefonica (prefisso internazionale, codice d'area, numero dell'abbonato)
  - Questo semplifica il lavoro nelle centrali di commutazione
- Gli indirizzi IPv4 invece non riflettono la gerarchia della rete Internet (in realtà tengono conto di un solo livello)
  - Conseguenza: le tabelle di routing crescono man mano che si sale verso i core router

21

## Aggregazione degli indirizzi



24

## Indirizzi unicast globali

- Gerarchia a 3 livelli:
  - Public Topology
  - Site Topology
  - Interface Identifier
- Public topology is the collection of providers and exchanges who provide public Internet transit services.
- Site topology is local to a specific site or organization which does not provide public transit service to nodes outside of the site.
- Interface identifiers identify interfaces on links.

25

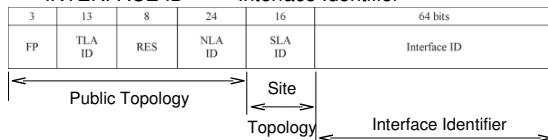
## Neighbor Discovery

- L'host diffonde un messaggio ICMPv6 di *richiesta del router*
  - Destinazione: gruppo multicast predefinito allo scopo
  - Sorgente: indirizzo IPv6 con prefisso link local unicast + 0..0 + indirizzo MAC (48 bit)
- Il router interessato risponde con un messaggio ICMPv6 di *annuncio del router* contenente il prefisso giusto per la rete
  - L'host completa il prefisso con il MAC ottenendo il proprio indirizzo IP

28

## Indirizzi unicast globali

- Hanno struttura che riflette la gerarchia della rete
  - FP Format Prefix (001)
  - TLA ID Top-Level Aggregation Identifier
  - RES Reserved for future use
  - NLA ID Next-Level Aggregation Identifier
  - SLA ID Site-Level Aggregation Identifier
  - INTERFACE ID Interface Identifier



26

## Capacità di instradamento avanzate: indirizzi anycast

- Sono normali indirizzi unicast
- Un gruppo di interfacce di host o router aventi la stessa funzionalità hanno lo stesso indirizzo unicast che prende il ruolo di indirizzo anycast
- Quando un client fa una richiesta diretta a tale indirizzo, essa viene servita dall'interfaccia più vicina
- Il concetto "più vicino" viene determinato dal routing
- Questa modalità permette la creazione di servizi ridondati per aumentarne la robustezza

29

## Autoconfigurazione

- Permette ad un host di ottenere un indirizzo IP in maniera dinamica
- IPv6 eredita la soluzione DHCP (Dynamic Host Configuration Protocol) a cui aggiunge una seconda tecnica chiamata *Neighbor Discovery* (ND)

27

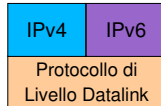
## Transizione da IPv4 a IPv6

- Transizione graduale
  - I nodi IPv4 continuano a colloquiare con nodi IPv4
  - I nodi IPv6 devono colloquiare con nodi IPv6 anche se i nodi interposti utilizzano solo IPv4
- Due soluzioni da combinare:
  - Operatività a doppia pila (dual stack operation)
  - Tunneling IPv6 in IPv4
  - Packet conversion from IPv4 to IPv6

30

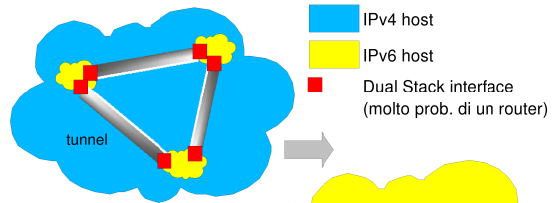
## Dual Stack Operation

- L'apparato ha sopra il Livello Datalink sia IPv4 sia IPv6
- Si utilizza il valore contenuto nel campo Version per decidere quale versione del livello network utilizzare



31

## Coesistenza tra IPv4 e IPv6



Nella conversione IPv4↔ IPv6 gli indirizzi IPv4 vengono convertiti in IPv6 mediante i due metodi visti prima. Tutti gli indirizzi IPv4 assegnati dalla IANA rimangono riservati in IPv6.

34

## Tunneling IPv6 in IPv4

- All'inizio del tunnel si incapsula il pacchetto IPv6 in un pacchetto IPv4 avente come sorgente e destinazione il nodo iniziale e terminale del tunnel, rispettivamente
- Al termine del tunnel si butta via il pacchetto IPv4 esterno
- I nodi iniziale e terminale del tunnel devono implementare la Dual Stack Operation e devono avere un programma di gestione del tunnel

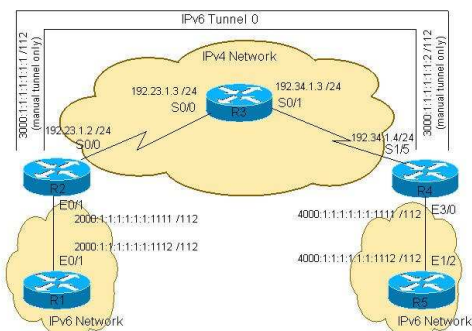
32

## Bibliografia

- IETF
  - RFC 2460-2466
  - <http://www.ietf.org/html.charters/6man-charter.html>
- <http://www.ipv6.org/>
- Wikipedia
  - <http://it.wikipedia.org/wiki/IPv6>
  - <http://en.wikipedia.org/wiki/IPv6>
- <http://www.it.ipv6tf.org/index.php>
- <http://www.ipv6forum.com/>
- Supporto per Linux
  - <http://www.pluto.it/files/ildp/HOWTO/Linux+IPv6-HOWTO/>

35

## Tunneling IPv6 in IPv4



33