



Università degli studi di Napoli Federico II
Facoltà di Scienze MM. FF. NN.
CdL in Informatica
a.a. 2001/2002

Montalto Paolo 50/278
Triunfo Maurizio 50/272

IPv6

Sistemi per l'elaborazione dell'informazione: Reti
Docente: Prof. Guido Russo

IPv6

Introduzione

La versione corrente di IP (nota come versione 4 o IPv4) non ha subito sostanziali modifiche dalla pubblicazione della RFC 791 nel 1981. IPv4 si è dimostrato essere un protocollo affidabile, di facile implementazione e interoperativo e ha superato la prova di scalabilità da una rete interna ad un'infrastruttura globale della portata di Internet, elemento fondamentale a conferma della validità del design originario.

Tuttavia, il design originario non prevedeva quanto segue:

- La recente crescita esponenziale di Internet e l'imminente esaurimento dello spazio degli indirizzi IPv4

Poiché gli indirizzi IPv4 sono divenuti relativamente scarsi, alcune organizzazioni si sono viste costrette ad utilizzare un NAT (Network Address Translator) per mappare più indirizzi privati ad un singolo indirizzo IP pubblico. I NAT favoriscono il riutilizzo dello spazio degli indirizzi privati, tuttavia non supportano la protezione del livello di rete standard né la mappatura corretta di tutti i protocolli di livello superiore e potrebbero dunque verificarsi problemi durante la connessione di due organizzazioni che utilizzano lo spazio degli indirizzi privati.

La crescente diffusione di dispositivi e congegni connessi ad Internet conferma inoltre che l'esaurimento dello spazio degli indirizzi IPv4 pubblici sarà inevitabile.

- L'espansione di Internet e la capacità dei router del backbone di Internet di gestire tabelle di routing di grandi dimensioni.

A causa del modo in cui gli ID di rete di IPv4 sono stati e sono attualmente allocati, le tabelle di routing dei router del backbone di Internet includono normalmente oltre 70.000 percorsi. L'attuale infrastruttura di routing Internet di IPv4 è una combinazione di entrambi i routing normale e gerarchico.

- La necessità di una configurazione più semplice

La maggior parte delle implementazioni correnti di IPv4 deve essere configurata manualmente o mediante un protocollo di configurazione degli indirizzi con gestione delle informazioni di stato quale DHCP (Dynamic Host Configuration Protocol). In presenza di più computer e dispositivi che utilizzano il protocollo IP, vi è la necessità di una configurazione degli indirizzi più semplice e più automatica e di altre impostazioni di configurazione che non dipendono dall'amministrazione di un'infrastruttura DHCP.

- I requisiti di sicurezza al livello IP

Le comunicazioni private su un mezzo pubblico quale Internet rendono necessari servizi di crittografia per la protezione dei dati inviati per impedirne la visualizzazione o la modifica durante il trasferimento. Sebbene attualmente esista uno standard per la protezione dei pacchetti IPv4 (noto come protezione IP o IPsec), tale standard è facoltativo e prevalgono soluzioni proprietarie.

- La necessità di un supporto migliore per l'invio di dati in tempo reale, definito anche qualità del servizio (QoS)

Sebbene esistano standard di QoS per IPv4, il supporto per il traffico in tempo reale si basa sul campo TOS (tipo di servizio) di IPv4 e sull'identificazione del payload, solitamente utilizzando una porta UDP o TCP. Sfortunatamente, il campo TOS di IPv4 dispone di una funzionalità limitata e ne sono state elaborate varie interpretazioni locali nel tempo. Inoltre, quando il payload del pacchetto IPv4 è crittografato, non è possibile effettuare l'identificazione del payload utilizzando una porta TCP o UDP.

Per affrontare questi problemi, la IETF (Internet Engineering Task Force) ha sviluppato un pacchetto di protocolli e standard noti come IP versione 6 (IPv6). Questa nuova versione, in un primo tempo denominata IPng (IP-The Next Generation), incorpora i concetti di numerosi metodi proposti per l'aggiornamento del protocollo IPv4. Il design di IPv6 è volutamente mirato a ridurre al minimo l'impatto sui protocolli di livello superiore e inferiore evitando l'aggiunta superflua di nuove funzionalità.

Funzionalità e caratteristiche di IPv6

Il protocollo IPv6 dispone delle seguenti funzionalità e caratteristiche:

- Nuovo formato dell'intestazione
- Spazio degli indirizzi esteso
- Infrastruttura di routing e di indirizzamento gerarchica ed efficiente
- Configurazione degli indirizzi con o senza gestione delle informazioni sullo stato (stateful, stateless)
- Sicurezza integrata
- Migliore supporto QoS
- Nuovo protocollo per l'interazione dei nodi adiacenti
- Estensibilità

Le sezioni che seguono contengono una descrizione dettagliata di ciascuna di queste nuove funzionalità e caratteristiche.

Nuovo formato dell'intestazione

L'intestazione di IPv6 dispone di un nuovo formato progettato per ridurre al minimo il sovraccarico correlato alle intestazioni, mediante il trasferimento dei campi non essenziali e facoltativi nelle intestazioni di estensione collocate dopo l'intestazione di IPv6. L'intestazione semplificata di IPv6 consente di ottenere un'elaborazione più efficiente in corrispondenza dei router intermedi.

Le intestazioni di IPv4 e di IPv6 non sono intercambiabili. È necessario che un host o un router utilizzi un'implementazione di entrambe le versioni per il riconoscimento e l'elaborazione di entrambi i formati di intestazione. Nonostante l'estensione della nuova intestazione di IPv6 sia soltanto il doppio di quella di IPv4, gli indirizzi IPv6 sono quattro volte più estesi di quelli IPv4.

Spazio degli indirizzi esteso

IPv6 dispone di indirizzi IP di origine e di destinazione a 128 bit (16 byte). Sebbene 128 bit possano generare oltre $3,4 \times 10^{38}$ combinazioni possibili, il vasto spazio degli indirizzi di IPv6 è stato progettato per consentire più livelli di subnetting e allocazione di indirizzi dal backbone di Internet alle singole subnet all'interno di un'organizzazione.

Sebbene solo un numero limitato degli indirizzi possibili sia attualmente allocato per l'utilizzo da parte degli host, vi è una grande quantità di indirizzi disponibili per un utilizzo futuro. Grazie al numero molto più vasto di indirizzi disponibili, le tecniche per la conservazione degli indirizzi, quali l'utilizzo di NAT, non sono più necessarie.

Infrastruttura di routing e di indirizzamento gerarchico ed efficiente

Gli indirizzi globali di IPv6 utilizzati nella parte di Internet riservata a IPv6 sono stati progettati per la creazione di un'infrastruttura di routing efficiente e gerarchica, basata sulla normale presenza di più livelli di provider di servizi Internet. Su Internet IPv6, i router di backbone dispongono di tabelle di routing notevolmente ridotte, che corrispondono all'infrastruttura di routing di aggregatori di livello superiore.

Configurazione degli indirizzi con o senza gestione delle informazioni sullo stato (stateful, stateless)

Per semplificare la configurazione host, IPv6 supporta la configurazione degli indirizzi sia con gestione di informazioni sullo stato, come nel caso della configurazione di indirizzi in presenza di un server DHCP, che senza informazioni sullo stato (configurazione di indirizzi in assenza di un server DHCP). Grazie alla configurazione degli indirizzi senza informazioni sullo stato, gli host su un collegamento vengono configurati automaticamente con indirizzi IPv6 per il collegamento (denominati indirizzi del collegamento locale) e con indirizzi derivati dai prefissi annunciati dai router locali. Anche in assenza di un router, gli host sullo stesso collegamento sono in grado di configurarsi automaticamente mediante indirizzi del collegamento locale e di comunicare senza interventi manuali di configurazione.

Sicurezza incorporata

Il supporto per IPSec è un requisito del pacchetto del protocollo IPv6. Tale requisito fornisce una soluzione standard per le esigenze di sicurezza della rete e promuove l'interoperabilità tra le diverse implementazioni di IPv6.

Migliore supporto QoS

I nuovi campi nell'intestazione IPv6 definiscono la modalità di gestione e identificazione del traffico. L'identificazione del traffico utilizzando un campo Etichetta del flusso nell'intestazione IPv6 consente ai router di identificare e impostare una gestione speciale per i pacchetti che appartengono a un flusso, ovvero una serie di pacchetti tra un'origine e una destinazione. Poiché il traffico viene identificato nell'intestazione IPv6, il supporto QoS può essere ottenuto anche nel caso in cui il payload del pacchetto sia stato crittografato utilizzando IPSec.

Nuovo protocollo per l'interazione dei nodi adiacenti

Il protocollo di rilevamento adiacente (ND, Neighbor Discovery) per IPv6 è costituito da una serie di messaggi ICMPv6 (Internet Control Message Protocol per IPv6) che

gestiscono l'interazione dei nodi adiacenti (nodi sullo stesso collegamento). Il protocollo di rilevamento adiacente sostituisce il protocollo ARP (Address Resolution Protocol) basato su broadcast, il protocollo di rilevamento router ICMPv4 e i messaggi di reindirizzamento ICMPv4 con messaggi ND efficienti unicast e multicast.

Estensibilità

IPv6 può essere esteso con facilità per accogliere nuove funzionalità mediante l'aggiunta di intestazioni di estensione dopo l'intestazione IPv6. Diversamente dalle opzioni nell'intestazione IPv4, che possono supportare solo 40 byte di opzioni, la dimensione delle intestazioni di estensione IPv6 è limitata esclusivamente dalla dimensione del pacchetto IPv6.

Differenze tra IPv4 e IPv6

Nella tabella 1 sono descritte alcune delle principali differenze tra IPv4 e IPv6.

Tabella 1 Differenze tra IPv4 e IPv6

IPv4	IPv6
Gli indirizzi di origine e destinazione dispongono di una lunghezza pari a 32 bit (4 byte).	Gli indirizzi di origine e di destinazione dispongono di una lunghezza pari a 128 bit (16 byte).
Il supporto IPsec è facoltativo.	Il supporto IPsec è necessario.
Nell'intestazione IPv4 non è prevista alcuna identificazione del payload per la gestione QoS da parte dei router.	L'identificazione del payload per la gestione QoS da parte dei router viene inclusa nell'intestazione IPv6 utilizzando il campo Etichetta del flusso.
La frammentazione è supportata presso i router e l'host di invio.	La frammentazione non è supportata presso i router, ma è supportata solo presso l'host di invio.
L'intestazione include un checksum.	L'intestazione non include un checksum.
L'intestazione include opzioni.	Tutti i dati opzionali vengono spostati nelle intestazioni di estensione IPv6.
Il protocollo ARP utilizza frame di richiesta ARP di broadcast per risolvere un indirizzo IPv4 in un indirizzo del livello di collegamento.	I frame di richiesta ARP vengono sostituiti con messaggi di richiesta del nodo adiacente multicast.
Il protocollo IGMP (Internet Group Management Protocol) è utilizzato per gestire l'appartenenza al gruppo di subnet locale.	Il protocollo IGMP viene sostituito con messaggi MLD (Multicast Listener Discovery).
Il protocollo di rilevamento router ICMP viene utilizzato per determinare l'indirizzo IPv4 del gateway predefinito migliore ed è facoltativo.	Il protocollo di rilevamento router ICMPv4 viene sostituito da messaggi di richiesta e di annuncio router ICMPv6 che sono obbligatori.
Gli indirizzi broadcast sono utilizzati per inviare il traffico a tutti i nodi di una subnet.	Non sono previsti indirizzi broadcast IPv6. Viene invece utilizzato un indirizzo multicast per tutti i nodi, locale per il collegamento.
È necessario eseguire la configurazione	Non è necessario eseguire la

manualmente o mediante DHCP.	configurazione manualmente né mediante DHCP.
Utilizza record di risorsa di indirizzi host (A) nel DNS (Domain Name System) per effettuare il mapping dei nomi host agli indirizzi IPv4.	Utilizza record di risorsa AAAA nel DNS per effettuare il mapping dei nomi host agli indirizzi IPv6.
Utilizza record di risorsa puntatore (PTR) nel dominio IN-ADDR.ARPA DNS per effettuare il mapping degli indirizzi IPv4 ai nomi host.	Utilizza record di risorsa puntatore (PTR) nel dominio DNS IP6.INT o IP6.ARPA per effettuare il mapping degli indirizzi IPv6 ai nomi host.
Deve supportare pacchetti con dimensione di 576 byte (con probabile frammentazione).	Deve supportare pacchetti con dimensione di 1280 byte (senza frammentazione).

Pacchetti IPv6 sui supporti LAN

Un frame del livello di collegamento contenente un pacchetto IPv6 è strutturato nel modo seguente:

- Intestazione e chiusura del livello di collegamento - L'incapsulamento inserito nel pacchetto IPv6 al livello di collegamento.
- Intestazione IPv6 - La nuova intestazione IPv6.
- Payload - Il payload (o segmento dati) del pacchetto IPv6.

La figura 1 illustra la struttura di un frame del livello di collegamento contenente un pacchetto IPv6.

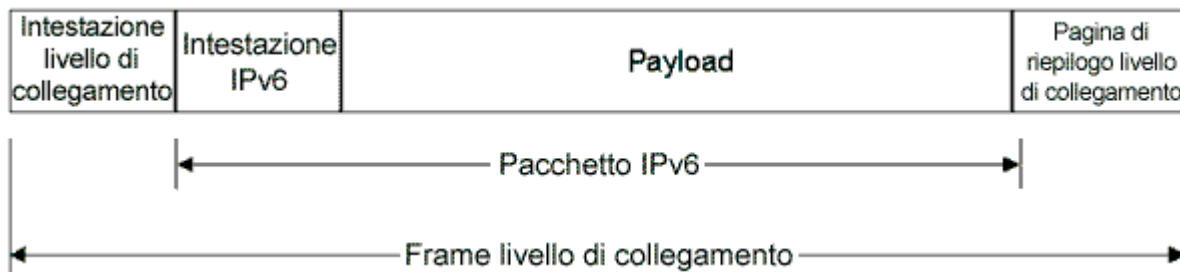


Figura 1 Pacchetti IPv6 al livello di collegamento

Per le tecnologie LAN tipiche, quali Ethernet, Token Ring e FDDI (Fiber Distributed Data Interface), i pacchetti IPv6 possono essere incapsulati in due modi, con l'intestazione Ethernet II o con un'intestazione SNAP (Sub-Network Access Protocol) utilizzata da IEEE 802.3 (Ethernet), IEEE 802.5 (Token Ring) e FDDI.

Indirizzi IPv6

Spazio degli indirizzi IPv6

La caratteristica distintiva più evidente di IPv6 è l'utilizzo di indirizzi più lunghi. La dimensione di un indirizzo IPv6 è pari a 128 bit, ovvero quattro volte superiore a quella di un indirizzo IPv4. Uno spazio degli indirizzi a 32 bit consente fino a 4.294.967.296 indirizzi possibili. Uno spazio a 128 bit consente fino a

340.282.266.920.938.463.463.374.607.431.768.211.465 (o $3,4 \times 10^{38}$)

indirizzi possibili.

Alla fine degli anni settanta, quando venne progettato lo spazio degli indirizzi IPv4, era addirittura impensabile che potesse arrivare ad esaurimento. Tuttavia, a causa dei progressi tecnologici e di una procedura di assegnazione che non prevedeva il recente straordinario sviluppo degli host su Internet, lo spazio degli indirizzi IPv4 si era ridotto a tal punto che già nel 1992 è emersa chiaramente la necessità di una soluzione alternativa.

Con IPv6, è molto difficile immaginare che lo spazio degli indirizzi IPv6 possa esaurirsi. Per meglio comprenderne la portata, si consideri che uno spazio degli indirizzi a 128 bit rende disponibili $655.570.793.348.866.943.898.599$ ($6,5 \times 10^{23}$) indirizzi per ogni metro quadrato della superficie terrestre.

La decisione di impostare una lunghezza di 128 bit per gli indirizzi IPv6 non deriva certamente dalla necessità di disporre di $6,5 \times 10^{23}$ indirizzi per ogni metro quadrato della terra. La dimensione relativamente estesa dell'indirizzo IPv6 è stata invece progettata per consentire la suddivisione in domini di routing gerarchici in grado di riflettere la topologia attuale di Internet. L'utilizzo di 128 bit consente più livelli di gerarchie e offre una maggiore flessibilità nella progettazione di strutture gerarchiche di indirizzamento e routing, attualmente non disponibile per Internet basata su IPv4.

L'architettura di indirizzamento IPv6 è descritta nella specifica RFC 2373.

Sintassi degli indirizzi IPv6

Gli indirizzi IPv4 sono espressi in formato decimale con punti. L'indirizzo a 32 bit è suddiviso in blocchi di 8 bit. Ogni serie di 8 bit viene convertita nel relativo equivalente decimale e separata da punti. Per IPv6, l'indirizzo a 128 bit è suddiviso in blocchi di 16 bit e ogni blocco a 16 bit viene convertito in un numero esadecimale a 4 cifre e separato da due punti. La rappresentazione che ne risulta è denominata "esadecimale con due punti".

Il seguente è un indirizzo IPv6 in formato binario:

```
0010000111011010100100001101001100000000010100000010111100111011
```

```
000000101010101000000000111111111111110001010001001110001011010
```

L'indirizzo a 128 bit è suddiviso in blocchi di 16 bit:

```
0010000111011010 1001000011010011 0000000001010000 0010111100111011  
0000001010101010 0000000011111111 1111111000101000 1001110001011010
```

Ogni blocco di 16 bit è convertito in esadecimale e delimitato dai due punti. Il risultato è:

```
21DA:00D3:0000:2F3B:02AA:00FF:FE28:9C5A
```

La rappresentazione IPv6 può essere ulteriormente semplificata rimuovendo gli zeri iniziali all'interno di ciascun blocco di 16 bit. Tuttavia, è necessario che ogni blocco includa

almeno una cifra. Con la rimozione degli zeri iniziali, la rappresentazione dell'indirizzo diventa:

21DA:D3:0:2F3B:2AA:FF:FE28:9C5A

Prefissi IPv6

Il prefisso è la parte dell'indirizzo che indica i bit con valori fissi o che rappresentano i bit dell'identificatore di rete. I prefissi IPv6 per gli identificatori di subnet e route sono espressi nello stesso modo della notazione CIDR (Classless Inter-Domain Routing) per IPv4. Un prefisso IPv6 viene scritto con la notazione *indirizzo/lunghezza_prefisso*. Ad esempio, 21DA:D3::/48 è un prefisso di route e 21DA:D3:0:2F3B::/64 è un prefisso di subnet. Le implementazioni IPv4 utilizzano normalmente una rappresentazione decimale con punti del prefisso di rete, nota come subnet mask. Per Ipv6 non viene utilizzata alcuna subnet mask. È supportata esclusivamente la notazione della lunghezza del prefisso.

Tipi di indirizzi IPv6

Esistono tre tipi di indirizzi IPv6:

1. Unicast

Un indirizzo unicast identifica una sola interfaccia all'interno dell'ambito del tipo di indirizzo unicast. Con la topologia di routing unicast appropriata, i pacchetti indirizzati a un indirizzo unicast vengono consegnati a un'interfaccia singola. Per le esigenze dei sistemi di bilanciamento del carico, la specifica RFC 2373 consente a più interfacce di utilizzare lo stesso indirizzo, purché appaiano come interfaccia singola all'implementazione Ipv6 sull'host.

2. Multicast

Un indirizzo multicast identifica più interfacce. Con la topologia di routing multicast appropriata, i pacchetti indirizzati a un indirizzo multicast vengono consegnati a tutte le interfacce identificate dall'indirizzo.

3. Anycast

Un indirizzo anycast identifica più interfacce. Con la topologia di routing appropriata, i pacchetti indirizzati a un indirizzo anycast vengono consegnati a un'interfaccia singola, quella più vicina identificata dall'indirizzo. L'interfaccia "più vicina" è definita in termini di distanza di routing. Per la comunicazione di tipo uno-a-molti con consegna a più interfacce viene utilizzato un indirizzo multicast. Per la comunicazione di tipo uno-a-uno con consegna a un'interfaccia singola viene utilizzato un indirizzo unicast. In tutti i casi, gli indirizzi IPv6 identificano le interfacce, non i nodi. Un nodo viene identificato da qualsiasi indirizzo unicast assegnato a una delle relative interfacce. Tutti i tipi di indirizzi broadcast IPv4 sono inesistenti in IPv6, tale lacuna è colmata facendo uso dell'indirizzamento multicast.

Collegamenti e subnet

Analogamente a IPv4, il prefisso di una subnet IPv6 (subnet ID) viene assegnato a un singolo collegamento. È possibile assegnare più subnet ID allo stesso collegamento. Questa tecnica è detta *multinetting*. Non è, come per IPv4, consentito assegnare un unico subnet ID a più collegamenti.

Indirizzi IPv6 speciali

Gli indirizzi riportati di seguito sono indirizzi IPv6 speciali:

- Indirizzo non specificato

L'indirizzo non specificato (0:0:0:0:0:0:0 oppure ::) viene utilizzato esclusivamente per indicare l'assenza di un indirizzo. Tale indirizzo equivale all'indirizzo non specificato IPv4 0.0.0.0. L'indirizzo non specificato viene solitamente utilizzato come indirizzo di origine per i pacchetti che tentano di verificare l'univocità di un indirizzo di prova. L'indirizzo non specificato non viene mai assegnato a un'interfaccia né utilizzato come indirizzo di destinazione.

- Indirizzo di loopback

L'indirizzo di loopback (0:0:0:0:0:0:0:1 o ::1) viene utilizzato per identificare un'interfaccia a circuito chiuso (loopback) e abilita il nodo per l'autoinvio di pacchetti. Tale indirizzo equivale all'indirizzo di loopback IPv4 127.0.0.1. I pacchetti indirizzati all'indirizzo di loopback non devono mai essere inviati su un collegamento né inoltrati da un router IPv6.

Indirizzi IEEE 802

Gli identificatori di interfaccia tradizionali per le schede di rete utilizzano un indirizzo a 48 bit denominato indirizzo IEEE 802. Tale indirizzo è composto da un ID di società a 24 bit (detto anche ID del produttore) e un ID di estensione a 24 bit (detto anche ID di scheda). La combinazione dell'ID di società, che viene assegnato in modo univoco a ciascun produttore di schede di rete, e dell'ID di scheda, che viene assegnato in modo univoco a ciascuna scheda di rete al momento dell'assemblaggio, produce un indirizzo a 48 bit globalmente univoco. Questo indirizzo a 48 bit è inoltre denominato indirizzo fisico, hardware o MAC (Media Access Control).

I bit definiti all'interno dell'indirizzo IEEE 802 sono i seguenti:

U/L (Universale/Locale) - Il bit accanto al bit di ordine inferiore del primo byte viene utilizzato per indicare se l'indirizzo è amministrato universalmente o localmente. Se il bit U/L è impostato su 0, significa che l'indirizzo è amministrato dall'IEEE, mediante la designazione di un ID di società univoco. Se il bit U/L è impostato su 1, l'indirizzo è amministrato localmente. L'amministratore di rete ha sostituito l'indirizzo di produzione specificandone uno diverso.

I/G (Individuale/Gruppo) - Il bit di ordine inferiore del primo byte viene utilizzato per indicare se l'indirizzo è un indirizzo individuale (unicast) o di gruppo (multicast). Se

impostato su 0, l'indirizzo è un indirizzo unicast. Se impostato su 1, l'indirizzo è un indirizzo multicast.

In un normale indirizzo di scheda di rete 802.x, i bit U/L e I/G sono impostati su 0 e corrispondono a un indirizzo MAC unicast amministrato universalmente.

Indirizzi IPv4 e IPv6 equivalenti

Nella tabella 2 sono elencati gli indirizzi IPv4 e i principi di indirizzamento e i relativi equivalenti in IPv6.

Tabella 2 Allocazione corrente dello spazio degli indirizzi IPv6

Indirizzo IPv4	Indirizzo IPv6
Classi degli indirizzi Internet	Non implementati in IPv6
Indirizzi multicast (224.0.0.0/4)	Indirizzi multicast IPv6 (FF00::/8)
Indirizzi di broadcast	Non implementati in IPv6
L'indirizzo non specificato è 0.0.0.0	L'indirizzo non specificato è ::
L'indirizzo di loopback è 127.0.0.1	L'indirizzo di loopback è ::1
Indirizzi IP pubblici	Indirizzi unicast globali aggregabili
Indirizzi IP privati (10.0.0.0/8, 172.16.0.0/12 e 192.168.0.0/16)	Indirizzi locali del sito (FEC0::/48)
Indirizzi configurati automaticamente (169.254.0.0/16)	Indirizzi locali del collegamento (FE80::/64)
Rappresentazione di testi: notazione decimale con punti	Rappresentazione di testi: formato esadecimale con due punti con soppressione degli zeri iniziali e compressione degli zeri. Gli indirizzi compatibili con IPv4 sono espressi in notazione decimale con punti.
Rappresentazione dei bit di rete: subnet mask in notazione decimale con punti o lunghezza del prefisso	Rappresentazione dei bit di rete: solo notazione con lunghezza del prefisso
Risoluzione dei nomi DNS: record di risorsa (A) di indirizzi host IPv4	Risoluzione dei nomi DNS: record di risorsa (AAAA) di indirizzi host IPv6.
Risoluzione inversa DNS: dominio IN-ADDR.ARPA	Risoluzione inversa DNS: dominio IP6.INT (RFC 1886) o IP6.ARPA (RFC 2874)

Intestazione IPv6

L'intestazione IPv6 è una versione semplificata dell'intestazione IPv4. In questa intestazione vengono eliminati i campi non necessari o utilizzati raramente e vengono aggiunti campi che forniscono un supporto di qualità superiore per il traffico in tempo reale. Una riepilogo delle caratteristiche dell'intestazione IPv4 è utile per semplificare la comprensione dell'intestazione IPv6.

Intestazione IPv4

Nella figura 2 è illustrata l'intestazione IPv4 descritta nella specifica RFC 791.

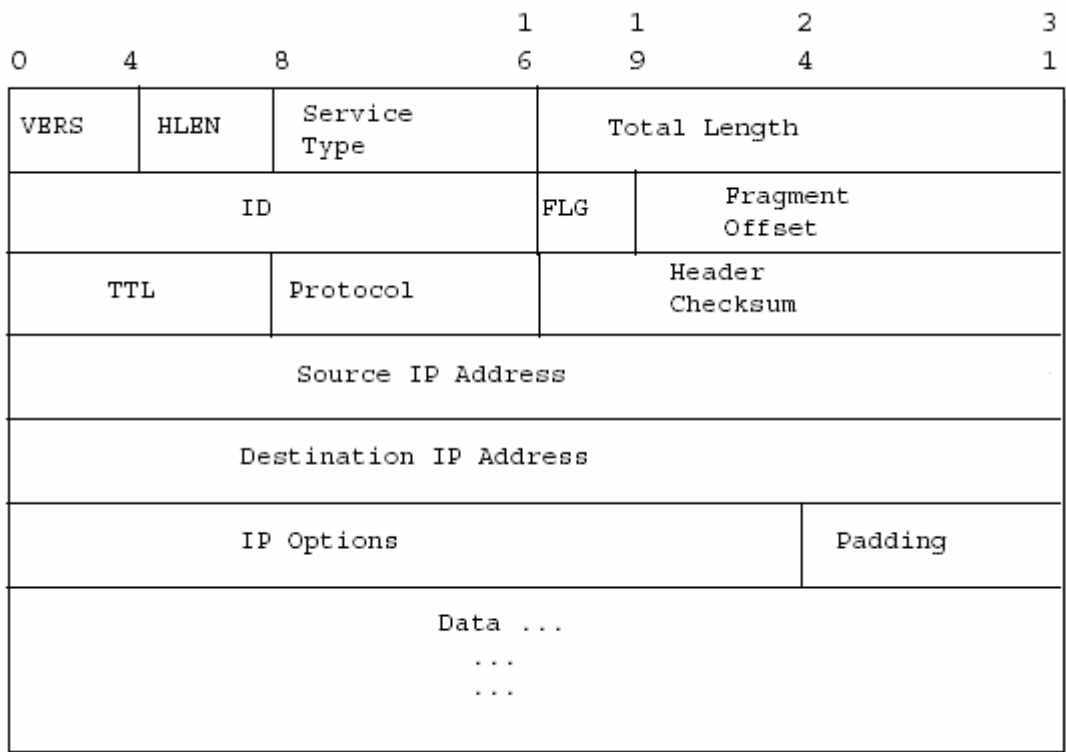


Figura 2 Intestazione IPv4

Di seguito vengono descritti i campi presenti nell'intestazione IPv4:

Versione - Indica la versione IP ed è impostato su 4. La dimensione di questo campo è pari a 4 bit.

Lunghezza intestazione Internet (HLEN) - Indica il numero dei blocchi di 4 byte presenti nell'intestazione IP. La dimensione di questo campo è pari a 4 bit. Poiché la dimensione minima di un'intestazione IP è di 20 byte, il valore minimo del campo HLEN (lunghezza intestazione) è 5. Tramite le opzioni IP è possibile estendere la dimensione minima dell'intestazione IP con incrementi di 4 byte. Se un'opzione IP non utilizza tutti i 4 byte del campo delle opzioni IP, i byte rimanenti vengono completati con 0, facendo in modo che l'intestazione IP diventi un numero integrale di 32 bit (4 byte). Con un valore massimo pari a 0xF, la dimensione massima dell'intestazione IP, incluse le opzioni, è di 60 byte (15*4).

Tipo di servizio - Indica il servizio desiderato per la consegna di questo pacchetto mediante i router sulla rete IP. La dimensione di questo campo è pari a 8 bit, che contengono bit per la precedenza, per il ritardo, per la velocità effettiva oltre a caratteristiche di affidabilità.

Lunghezza totale - Indica la lunghezza totale del pacchetto IP (intestazione IP + payload IP) e non include frame del livello di collegamento. La dimensione di questo campo è di 16 bit, che possono indicare un pacchetto IP con una lunghezza massima pari a 65.535 byte.

Identificazione - Identifica un pacchetto IP specifico. La dimensione di questo campo è pari a 16 bit. Il campo di identificazione viene selezionato dall'origine del pacchetto IP. Se il pacchetto IP è frammentato, tutti i frammenti mantengono il valore del campo di

identificazione in modo che il nodo di destinazione possa raggrupparli per il riassetto.

Flag - Identifica i flag per il processo di frammentazione. La dimensione di questo campo è di 3 bit, tuttavia, per l'utilizzo corrente vengono definiti solo 2 bit. Esistono due flag: uno che indica se il pacchetto IP può essere frammentato e un altro che indica se il frammento corrente è seguito da più frammenti.

Offset del frammento - Indica la posizione del frammento relativa al payload IP originale. La dimensione di questo campo è pari a 13 bit.

Durata (TTL) - Indica il numero massimo di collegamenti su cui un pacchetto IP può viaggiare prima di essere scartato. La dimensione di questo campo è pari a 8 bit. Il campo di durata (TTL, Time-to-Live) era originariamente utilizzato come contatore temporale mediante il quale un router IP era in grado di determinare la quantità di tempo necessaria (in secondi) per inoltrare il pacchetto IP, producendo di conseguenza una diminuzione del TTL. I router moderni sono quasi sempre in grado di inoltrare un pacchetto IP in meno di un secondo e secondo la specifica RFC 791 devono diminuire il TTL di almeno una unità. Il TTL diventa pertanto un contatore di collegamenti massimi con il valore impostato dal nodo di invio. Se il TTL è pari a 0, il pacchetto viene scartato e un messaggio di tempo scaduto ICMP viene inviato all'indirizzo IP di origine.

Protocollo - Identifica il protocollo di livello superiore. La dimensione di questo campo è pari a 8 bit. Ad esempio, TCP utilizza un protocollo 6, UDP un protocollo 17 e ICMP un protocollo 1. Il campo del protocollo viene utilizzato per il demultiplex di un pacchetto IP al protocollo di livello superiore.

Checksum intestazione - Fornisce un checksum solo per l'intestazione IP. La dimensione di questo campo è pari a 16 bit. Il calcolo di checksum non include il payload IP in quanto quest'ultimo solitamente contiene il proprio checksum. Ogni nodo IP che riceve pacchetti IP verifica il checksum dell'intestazione e scarta automaticamente il pacchetto in caso di esito negativo della verifica del checksum. Quando un router inoltra un pacchetto IP è necessario che diminuisca il TTL. Pertanto, il checksum dell'intestazione viene ricalcolato ad ogni passaggio tra l'origine e la destinazione.

Indirizzo di origine - Contiene l'indirizzo IP dell'host di origine. La dimensione di questo campo è pari a 32 bit.

Indirizzo di destinazione - Contiene l'indirizzo IP dell'host di destinazione. La dimensione di questo campo è pari a 32 bit.

Opzioni - Contiene una o più opzioni IP. La dimensione di questo campo è un multiplo di 32 bit. Se l'opzione o le opzioni IP non utilizzano tutti i 32 bit, devono essere aggiunte opzioni di riempimento in modo che l'intestazione IP sia un numero integrale di 4 byte che può essere indicato dal campo HLEN.

Riempimento (Padding) - Se è utilizzata un'opzione, il pacchetto viene riempito di byte a zero fino al prossimo limite dei 32 bit.

Struttura di un pacchetto IPv6

Intestazione IPv6

L'intestazione IPv6 è sempre presente e dispone di una dimensione fissa pari a 40 byte.

Nella figura 3 è illustrata la struttura di un pacchetto IPv6.

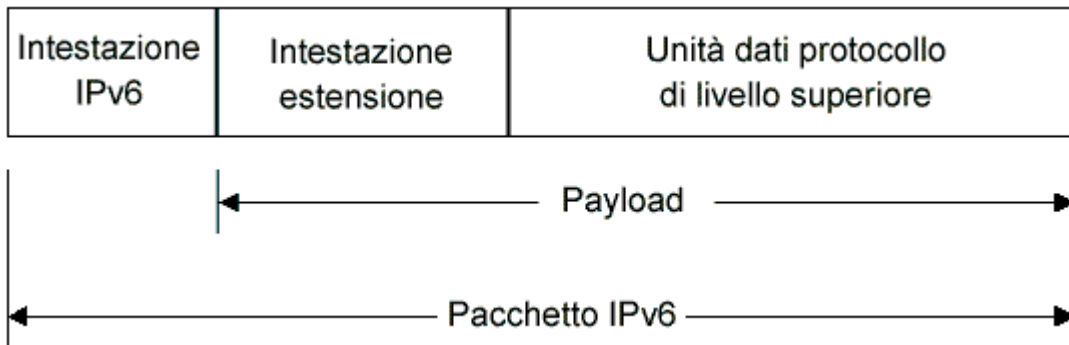


Figura 3 Struttura di un pacchetto IPv6

Intestazioni di estensione

Possono essere presenti zero o più intestazioni di estensione di lunghezza variabile. Un campo Intestazione successiva (Next Header) nell'intestazione IPv6 indica l'intestazione di estensione successiva. All'interno di ciascuna intestazione di estensione si trova un altro campo Intestazione successiva che indica l'intestazione di estensione successiva. L'ultima intestazione di estensione indica il protocollo di livello superiore (TCP, UDP o ICMPv6) contenuto nell'unità dati del protocollo di livello superiore.

L'intestazione IPv6 e le intestazioni di estensione sostituiscono l'intestazione IP IPv4 esistente con opzioni. Il nuovo formato dell'intestazione di estensione consente di potenziare IPv6 per il supporto di necessità e volumi futuri. Diversamente dalle opzioni dell'intestazione IPv4, per le intestazioni di estensione IPv6 non è prevista una dimensione massima e possono perciò espandersi in modo da accogliere tutti i dati di estensione necessari per le comunicazioni IPv6.

Unità dati del protocollo di livello superiore (PDU)

L'unità dati del protocollo di livello superiore (PDU) è solitamente composta da un'intestazione del protocollo di livello superiore e dal relativo payload (ad esempio, un messaggio ICMPv6, un messaggio UDP o un segmento TCP).

Il payload del pacchetto IPv6 è dato dalla combinazione delle intestazioni di estensione IPv6 e del PDU di livello superiore. Normalmente, tale payload può avere una lunghezza massima di 65.535 byte. I payload di lunghezza superiore possono essere inviati utilizzando l'opzione Payload jumbo nell'intestazione di estensione delle opzioni hop-by-hop.

Intestazione IPv6

Nella figura 4 è illustrata l'intestazione IPv6 definita nella specifica RFC 2460.

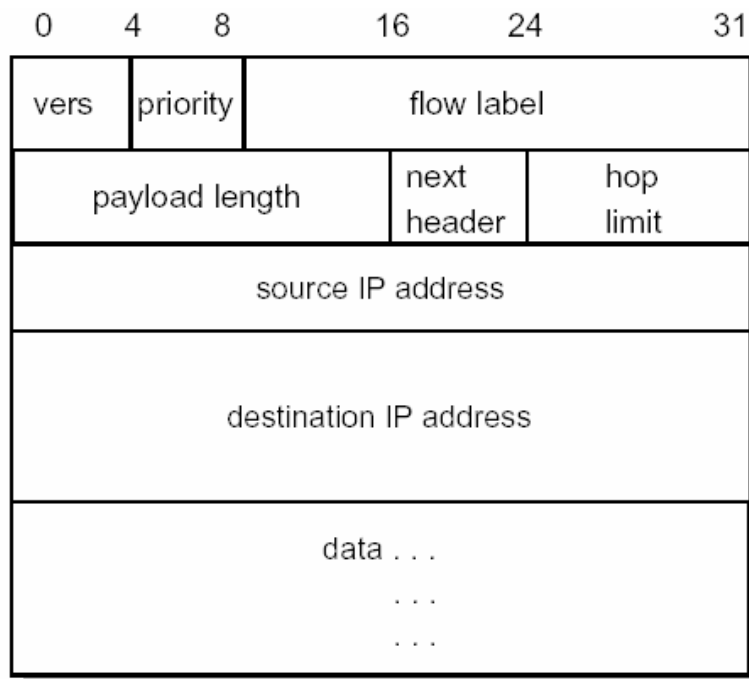


Figura 4 Intestazione IPv6

Di seguito sono riportati i campi presenti nell'intestazione IPv6:

Versione - In questo campo sono utilizzati 4 bit per indicare la versione di IP ed è impostato su 6.

Classe di traffico (Priority) - Indica la classe o la priorità del pacchetto IPv6. La dimensione di questo campo è pari a 8 bit. Il campo Classe di traffico fornisce funzionalità simili a quelle del campo Tipo di servizio di IPv4. I valori del campo Classe di traffico non sono definiti nella specifica RFC 2460. Un'implementazione IPv6 è tuttavia necessaria per fornire un mezzo attraverso il quale un protocollo del livello applicazione sia in grado di specificare il valore del campo Classe di traffico per la sperimentazione.

Etichetta flusso (flow label)- Indica che il presente pacchetto appartiene a una sequenza specifica di pacchetti tra un'origine e una destinazione e che richiede una gestione speciale da parte dei router IPv6 intermedi. La dimensione di questo campo è pari a 20 bit. Il campo Etichetta flusso viene utilizzato per connessioni di qualità di servizio (QoS) non predefinite, come quelle necessarie per i dati in tempo reale (voce e video). Per la gestione dei router predefiniti, il campo Etichetta flusso è impostato su 0. Possono esistere più flussi tra un'origine e una destinazione, contraddistinti da etichette di flusso separate diverse da zero.

Lunghezza payload - Indica la lunghezza del payload IP. La dimensione di questo campo è pari a 16 bit. Il campo Lunghezza payload include le intestazioni di estensione e il PDU di livello superiore. Con 16 bit è possibile indicare un payload IPv6 di un massimo di 65.535 byte. Per i payload di lunghezza superiore a 65.535 byte, il campo Lunghezza

payload è impostato su 0 e l'opzione Payload jumbo viene utilizzata nell'intestazione di estensione delle opzioni hop-by-hop.

Intestazione successiva (next header) - Indica la prima intestazione di estensione (se presente) o il protocollo nella PDU di livello superiore (TCP, UDP o ICMPv6). La dimensione di questo campo è pari a 8 bit.

Limite hop - Indica il numero massimo di collegamenti sui quali il pacchetto IPv6 può viaggiare prima di essere scartato. La dimensione di questo campo è pari a 8 bit. Il campo Limite hop è simile al campo di durata (TTL) IPv4 ad eccezione del fatto che non vi è alcuna relazione con la quantità di tempo (in secondi) in cui il pacchetto rimane in coda al router. Quando Limite hop è pari a 0, il pacchetto viene scartato e un messaggio ICMP di tempo scaduto viene inviato all'indirizzo di origine.

Indirizzo di origine - Contiene l'indirizzo IPv6 dell'host di origine. La dimensione di questo campo è pari a 128 bit.

Indirizzo di destinazione - Contiene l'indirizzo IPv6 dell'host di destinazione corrente. La dimensione di questo campo è pari a 128 bit. Nella maggior parte dei casi, l'indirizzo di destinazione è impostato sull'indirizzo di destinazione finale. Tuttavia, in presenza di un'intestazione di estensione del routing, potrebbe essere impostato sull'interfaccia di router successiva nell'elenco di routing di origine.

Configurazione automatica degli indirizzi : DHCP

Uno degli aspetti maggiormente utili di IPv6 è la capacità di configurazione automatica, anche senza utilizzare un protocollo di configurazione con gestione delle informazioni sullo stato come DHCPv6. Per impostazione predefinita, un host IPv6 è in grado di effettuare la configurazione di un indirizzo locale del collegamento per ogni interfaccia. Mediante il meccanismo di rilevamento del router, un host è inoltre in grado di determinare gli indirizzi dei router, altri parametri di configurazione, gli indirizzi aggiuntivi e i prefissi on-link. In un messaggio di annuncio del router è inclusa l'indicazione relativa all'eventuale necessità di un protocollo di configurazione degli indirizzi con gestione delle informazioni sullo stato.

La configurazione automatica degli indirizzi può essere eseguita esclusivamente su interfacce che supportano il multicast. La configurazione automatica degli indirizzi è descritta nella specifica RFC 2462.

IPv6 e DNS

Nelle due specifiche seguenti sono descritti i miglioramenti apportati al sistema DNS (Domain Name System) per IPv6:

- RFC 1886: "DNS Extensions to support IP version 6"
- RFC 2874: "DNS Extensions to Support IPv6 Address Aggregation and Renumbering"

Supporto RFC 1886

In base alla specifica RFC 1886, per la risoluzione di un nome di dominio completo in un indirizzo IPv6 viene utilizzato un nuovo tipo di record di risorsa DNS, AAAA (denominato "quad A"). È possibile paragonare tale tipo di record al record di risorsa degli indirizzi host

(A) utilizzato con IPv4. Questo tipo di record di risorsa è denominato AAAA (valore del tipo pari a 28) in quanto gli indirizzi IPv6 a 128 bit sono quattro volte più grandi degli indirizzi IPv4 a 32 bit. Di seguito viene riportato un esempio di record di risorsa AAAA:

```
host1.microsoft.com      IN AAAA      FEC0::2AA:FF:FE3F:2A1C
```

Per poter ricevere i dati di risoluzione degli indirizzi IPv6 nelle sezioni di risposta alle query DNS, è necessario che un host specifichi una query AAAA o una query generale per un nome di host specifico.

La specifica RFC 1886 descrive inoltre il dominio IP6.INT creato per le query inverse IPv6. Chiamate anche query del puntatore, le query inverse determinano un nome di host in base all'indirizzo IP. Per creare lo spazio dei nomi delle query inverse, ogni cifra esadecimale dell'indirizzo IPv6 a 32 cifre espresso per esteso diventa un livello separato in ordine inverso all'interno della gerarchia del dominio inverso.

Il supporto DNS descritto nella specifica RFC 1886 non fornisce un metodo semplice per la diffusione delle modifiche dei record AAAA, a causa della rinumerazione dei siti o della delega delle zone di ricerca inversa sui confini dei bit arbitrari. La soluzione di questi problemi è descritta nella specifica RFC 2874.

Supporto RFC 2874

La specifica RFC 2874 risolve le limitazioni della RFC 1886, fondamentalmente è una trasposizione diretta delle tecniche di risoluzione dei nomi e degli indirizzi IPv4 per gli indirizzi IPv6. Con IPv6, i progettisti di DNS intendono risolvere alcuni dei problemi esistenti (anche nel DNS IPv4) in relazione alla rinumerazione dei siti. Se un'organizzazione cambia il provider di servizi Internet (ISP) e gli indirizzi IP pubblici, è necessario modificare moltissimi record DNS (sia indirizzi che record PTR). Un'altra limitazione della specifica RFC 1886 è rappresentata dal meccanismo dello spazio dei nomi con risoluzione inversa basato sui confini delle cifre esadecimali (nibble). Come già indicato, IPv6 e i prefissi degli indirizzi consentono una flessibilità a livello di bit e tale flessibilità deve essere disponibile anche per lo spazio dei nomi inverso. Per risolvere tali problemi, nella RFC 2874 è previsto l'utilizzo dei seguenti elementi:

- Un tipo di record detto A6 che sostituisce il record AAAA definito nella RFC 1886. Il record A6 consente di rendere disponibile un semplice mapping nome-indirizzo o il reindirizzamento a un altro nome DSN corrispondente a un prefisso di indirizzo. Tale reindirizzamento consente di suddividere lo spazio degli indirizzi di un dato indirizzo in record separati corrispondenti alla gerarchia di indirizzamento. La risoluzione del nome viene completata dopo la composizione di tutte le parti dell'indirizzo.
- Una nuova etichetta DNS denominata "etichetta bit-stringa" e descritta nella RFC 2673. Le etichette bit-stringa supportano una rappresentazione più sintetica per i mapping di indirizzi inversi.
- Un nuovo record di risorsa per la delega dello spazio degli indirizzi DNS denominato record DNAME.
- Un nuovo dominio inverso denominato IP6.ARPA.

ICMPv6

Analogamente a IPv4, IPv6 non fornisce funzioni per la segnalazione di errori, ma utilizza una versione aggiornata del protocollo ICMP (Internet Control Message Protocol) denominato ICMP versione 6 (ICMPv6). ICMPv6 dispone delle comuni funzioni ICMP IPv4

di segnalazione degli errori di consegna o di inoltra e fornisce un semplice servizio di eco per la risoluzione dei problemi.

Il protocollo ICMPv6 prevede inoltre un'infrastruttura per quanto segue:

- Rilevamento listener multicast MLD (multicast listener detect)

MLD è costituito da una serie di tre messaggi ICMP che sostituiscono la versione 2 del protocollo IGMP (Internet Group Management Protocol) per IPv4, per la gestione dell'appartenenza multicast delle subnet.

- ND (rilevamento nodo adiacente)

Il rilevamento ND è costituito da una serie di cinque messaggi ICMPv6 che gestiscono la comunicazione tra i nodi di un collegamento. Il rilevamento dei nodi adiacenti sostituisce il protocollo ARP (Address Resolution Protocol), il rilevamento router ICMPv4 e il messaggio di reindirizzamento ICMPv4.

ICMPv6 è necessario per un implementazione IPv6 ed è trattato nella specifica RFC2463.

Tipi di messaggi ICMPv6

Esistono due tipi di messaggi ICMPv6:

1. Messaggi di errore

I messaggi di errore vengono utilizzati per la segnalazione degli errori di inoltra o consegna dei pacchetti IPv6 da parte del nodo di destinazione o di un router intermedio. Nei messaggi di errore ICMPv6, il valore del campo di tipo a 8 bit è compreso tra 0 e 127 (il bit di ordine superiore è impostato su 0). I messaggi di errore ICMPv6 includono i messaggi che indicano la **destinazione non raggiungibile**, le **dimensioni eccessive del pacchetto**, il **tempo scaduto** e gli **errori di parametro**.

- 1 Destination Unreachable
- 2 Packet Too Big
- 3 Time (Hop Count) Exceeded
- 4 Parameter Problem

2. Messaggi informativi

I messaggi informativi vengono utilizzati per fornire funzioni diagnostiche e funzionalità host aggiuntive quali MLD e ND. Nei messaggi informativi ICMPv6, il valore del campo di tipo è compreso tra 128 e 255 (il bit di ordine superiore è impostato su 1). I messaggi informativi ICMPv6 sono descritti nella specifica RFC 2463 e includono **richiesta echo** e **risposta echo**.

- 128 Echo Request
- 129 Echo Reply
- 130 Group Membership Query
- 131 Group Membership Report
- 132 Group Membership Reduction
- 133 Router Solicitation
- 134 Router Advertisement
- 135 Neighbor Solicitation
- 136 Neighbor Advertisement
- 137 Redirect Message

BIBLIOGRAFIA

- [1] Silvano Gai, Pier Luca Montessoro, Pietro Nicoletti “ Reti locali: dal cablaggio all'internetworking”.
- [2] Martin W. Murhammer, Orcun Atakan, Stefan Bretz, Larry R. Pugh, Kazunari Suzuki, David H. Wood, “IBM TCP/IP tutorial and technical overview”.
- [3] Richard W. Stevens “UNIX – dal software all'internetworking”.
- [4] Silvano Gai “IPv6 alias IPng: un futuro per Internet e le Intranet”.