Azzolini Riccardo 2020-11-03

Internet Protocol

1 Internet Protocol

Internet Protocol (**IP**) è il principale protocollo di livello 3 (rete) della pila TCP/IP. Esso è responsabile dell'instradamento nella rete dei pacchetti, che a questo livello prendono il nome **datagrammi**, poiché IP offre un servizio connectionless inaffidabile, **best effort**, ovvero appunto *a datagramma*: non si ha alcuna garanzia che i pacchetti arrivino a destinazione, né tanto meno che vengano consegnati in ordine, senza duplicati, ecc.

Ogni datagramma IP contiene gli **indirizzi IP** del mittente e del destinatario. I dispositivi di relaying di livello 3, che sono i **router**, usano degli appositi **algoritmi di routing** per inoltrare ciascun datagramma ricevuto in base al suo indirizzo di destinazione, secondo il paradigma store and forward.

Quando si ha una comunicazione tra due host situati in reti diverse, i datagrammi IP possono essere trasferiti attraverso più reti, compiendo vari **hop** (salti) da un router al successivo, fino a raggiungere il destinatario. Se invece la comunicazione avviene tra host posti nella stessa rete, essa può avvenire direttamente tramite gli switch di tale rete, senza bisogno di router.

2 Indirizzi IP

Un indirizzo IP — nella versione 4 del protocollo, IPv4, che è attualmente la più diffusa — è composto da 32 bit, e viene tipicamente rappresentato in notazione *decimale puntata* (ad esempio 193.204.59.56). I 32 bit di un indirizzo IP sono suddivisi in due porzioni: un **net-id**, che identifica una rete, e un **host-id**, che identifica un host all'interno della rete.

Esistono cinque classi di indirizzi IP: A, B, C, D ed E. Ciascuna classe comprende uno specifico intervallo di indirizzi, e assegna agli indirizzi in questo intervallo un certo significato:

- le classi A, B e C stabiliscono diverse ripartizioni dei bit degli indirizzi tra net-id e host-id;
- la classe D contiene gli indirizzi usati per il *multicast*;
- la classe E è riservata per usi futuri.

Inoltre, anche all'interno di ciascuna di queste classi esistono indirizzi riservati per scopi specifici, come ad esempio il *broadcast*, che sono identificati da numeri particolari.

L'assegnazione di un indirizzo IP a un host può essere statica o dinamica:

- Un indirizzo **statico** se questo non varia nel tempo.
- Un indirizzo **dinamico**, al contrario, varia nel tempo. Ad esempio, se un utente ha una connessione non permanente a Internet, ogni volta che si connette riceve tipicamente dall'*ISP* (*Internet Service Provider*, il gestore del servizio di accesso a Internet) un qualche indirizzo IP tra quelli disponibili, e la scelta di indirizzo può cambiare di volta in volta.

L'ente che gestisce l'assegnazione degli indirizzi IP è la **IANA**, *Internet Assigned Numbers Authority*.

2.1 Indirizzi pubblici e privati

Un indirizzo IP può essere **pubblico** o **privato**:

- gli indirizzi pubblici sono quelli usati per instradare i pacchetti in Internet, e devono perciò essere assegnati in modo univoco;
- gli indirizzi privati possono essere usati solo in una rete privata, mentre non si possono instradare pacchetti con tali indirizzi in Internet.

La necessità degli indirizzi privati deriva principalmente dal fatto che lo *spazio degli indirizzi* IPv4 è troppo piccolo: con una lunghezza di 32 bit, esistono solo 2^{32} diversi indirizzi (circa 4 miliardi), che sono ormai esauriti (già tutti assegnati). È allora impensabile dare un indirizzo pubblico a ogni macchina in una rete. Invece, ogni macchina può tranquillamente avere un indirizzo privato, dato che questo è riutilizzabile senza problemi in reti diverse.

Per consentire poi alle macchine in una rete di comunicare con il resto di Internet, si assegna alla rete un singolo indirizzo pubblico (o comunque pochi), e si predispone al confine della rete un meccanismo di traduzione tra indirizzi pubblici e privati, chiamato NAT (Network Address Translation).

Come altra soluzione al problema della scarsità degli indirizzi, è stata sviluppata una nuova versione di IP, chiamata IPv6, che usa indirizzi di 128 bit. Tuttavia, nonostante sia pronto da parecchi anni, IPv6 rimane tuttora meno diffuso di IPv4.

2.2 Subnetting

All'interno degli indirizzi IP usati in una rete, una parte dei bit adibiti all'identificazione dell'host possono invece essere dedicati alla definizione di diverse **sottoreti** (**subnet**), tramite un identificatore che prende il nome di **subnet-id**.

Il numero di bit assegnati al subnet-id determina quante diverse sottoreti possono essere identificate: ad esempio, usando subnet-id di 3 bit possono essere definite $2^3 = 8$ sottoreti.[1]

I bit dedicati a net-id e subnet-id sono indicati dalla *subnet mask*, che viene solitamente indicata scrivendo il numero di questi bit dopo l'indirizzo IP, separato da una barra. Ad esempio, 193.204.59.56/24 indica che il net-id e il subnet-id sono composti complessivamente da 24 bit (quindi restano $32 - 24 = 8$ bit per l'host-id).

3 Address Resolution Protocol

Quando un host vuole stabilire una comunicazione a livello 3 con un altro host situato nella stessa rete, ha bisogno sia dell'indirizzo IP che dell'indirizzo MAC del destinatario, ma potrebbe essere che invece sappia solo l'indirizzo IP.

L'**Address Resolution Protocol**, **ARP**, permette proprio di conoscere l'indirizzo MAC corrispondente a un determinato indirizzo IP:

1. Un host A che conosce l'IP di un altro host B, e vuole saperne l'indirizzo MAC, invia in *broadcast* un messaggio di **ARP request**, che contiene l'indirizzo IP di B.

2. Quando B riceve questo messaggio, vede che l'indirizzo IP in esso contenuto è il suo, quindi risponde in *unicast* ad A, inviando una **ARP reply** contenente il proprio indirizzo MAC.

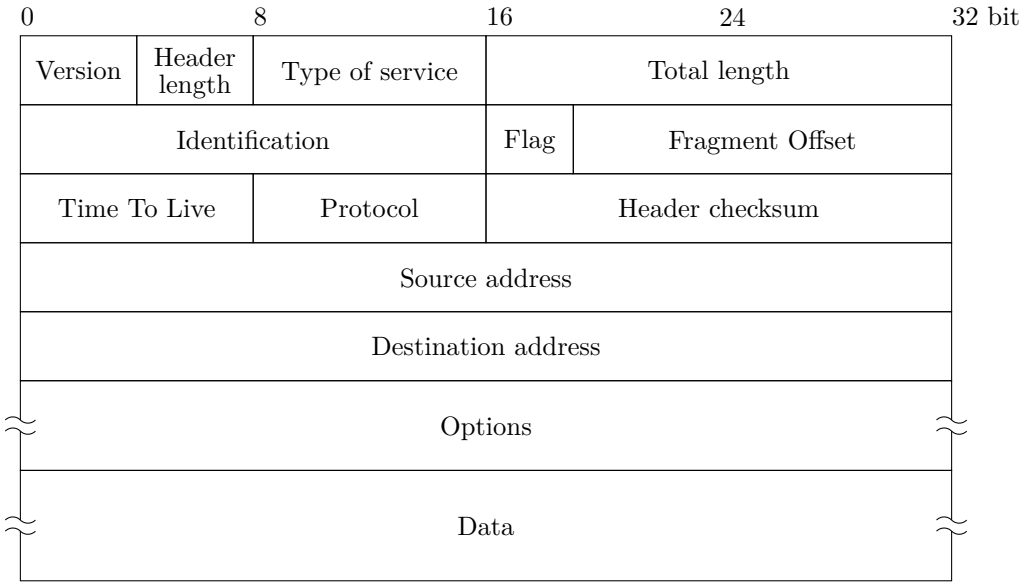
   Invece, tutti gli altri host sulla rete ignorano semplicemente la richiesta, vedendo che l'indirizzo IP specificato in tale richiesta non è il loro.

Per evitare di dover fare continuamente richieste ARP, ogni host ha una cache in cui memorizza i risultati delle richieste più recenti.

[1] Alcuni vecchi router non riconoscono i subnet-id aventi i bit tutti a 0 (000) oppure tutti a 1 (111): allora, con 3 bit sarebbero possibili solo $2^3 - 2 = 6$ sottoreti.

4 Datagramma IP

Il datagramma IPv4 è composto dai seguenti campi:



- **Version**: definisce la versione del protocollo (4 o 6).
- **Header length**: la dimensione dell'header, misurata in parole da 32 bit, cioè 4 byte. Ad esempio, per un header di 20 byte (che è la lunghezza minima), questo campo assume valore $\frac{20}{4} = 5$.
- **Type of service**: definisce i requisiti di QoS per il datagramma.
- **Total length**: la lunghezza complessiva del datagramma (header e dati), misurata in byte.
- **Identification**: identifica in modo univoco un datagramma generato dall'host mittente.
- **Flag**: questo campo contiene due bit di informazioni utili alla frammentazione (e un terzo bit riservato per usi futuri):
  - **DF**, *Don't Fragment*, se impostato, indica che il datagramma non può essere frammentato;
  - **MF**, *More Fragments*, indica che questo datagramma è un frammento di un datagramma originale più grande, e in particolare che non è l'ultimo frammento.

- **Fragment offset**: quando il datagramma è un frammento di un datagramma originale più grande, questo campo indica la posizione del primo byte di dati di questo frammento all'interno della sequenza di dati del datagramma originale, misurata in multipli di 8 byte. Ad esempio, un valore di offset pari a 185 indica che questo frammento contiene una porzione di dati a partire dal byte numero 1480 $(185 \cdot 8)$ del datagramma originale.

  Se il datagramma non è un frammento, il fragment offset è impostato a 0.
- **Time To Live** (**TTL**): un numero che viene decrementato di un'unità a ogni hop (passaggio da un router al successivo) che il datagramma compie. Quando il TTL raggiunge 0, il datagramma è scartato, per evitare che continui all'infinito a girare nella rete. Tipicamente, il mittente imposta inizialmente il TTL al valore 128.
- **Protocol**: indica il protocollo impiegato al livello 4 per questa comunicazione. Ad esempio, il valore 6 rappresenta TCP, mentre il valore 17 indica UDP.
- **Header checksum**: dei bit per il controllo dell'integrità dell'header.
- **Source address**: l'indirizzo IP dell'host mittente.
- **Destination address**: l'indirizzo IP dell'host destinatario.
- **Options**: opzioni per il routing del datagramma.
- **Data**: la SDU di livello 3, corrispondente alla PDU di livello 4.

4.1 Frammentazione

La SDU di livello data link ha una dimensione massima, chiamata **Maximum Transfer Unit** (**MTU**), che varia a seconda del tipo di rete, ecc. Siccome i datagrammi (PDU) IP devono rientrare in tale SDU, essi sono limitati a questa stessa dimensione massima.

Il mittente trasmette inizialmente un datagramma che rientra nell'MTU della *propria* rete, ma potrebbe accadere che un router si trovi a inoltrarlo su una rete che invece ha una MTU minore. Allora, tale datagramma deve essere **frammentato**, suddividendolo in frammenti più piccoli, che verranno poi riassemblati dall'host destinatario.

4.1.1 Esempio

Si supponga di dover inoltrare, su una rete con una MTU di 1500 byte, un datagramma che invece misura 4000 byte, di cui 20 byte costituiscono l'header e 3980 byte sono invece i dati (la SDU di livello 3). Sia 777 l'ID di questo datagramma.

Ogni frammento generato dal router dovrà contenere ancora un header di 20 byte, lasciando così un massimo di $1500 - 20 = 1480$ byte per i dati. Il datagramma di 4000 byte verrà allora suddiviso nei seguenti frammenti:

1. Un primo datagramma di 1500 byte che ha ID 777, offset 0 e il flag MF (More Fragments) impostato a 1. Esso contiene il solito header di 20 byte, e i 1480 byte di dati dal numero 0 al 1479.
2. Un secondo datagramma di 1500 byte, che ha lo stesso ID 777, un offset pari a 185, e MF a 1. L'offset 185 indica che questo datagramma contiene i byte della SDU originale a partire dal numero 1480 ($185 \cdot 8$); siccome anche in questo datagramma ci stanno 1480 byte di dati, l'ultimo byte incluso sarà il numero 2959.
3. Un ultimo datagramma contenente i byte restanti, che ha ID 777, offset 370 e il flag MF azzerato (perché non ci sono ulteriori frammenti). Questo contiene i byte di dati dal numero 2960 ($370 \cdot 8$) al numero 3979 (l'ultimo del datagramma originale). Ci sono allora 1020 byte di dati, che insieme all'header di 20 byte determinano una lunghezza complessiva del datagramma di 1040 byte.

L'ID rimane lo stesso, 777, in tutti i frammenti, in modo che il destinatario possa riconoscerli come parti del singolo datagramma originale.

5 Dynamic Host Configuration Protocol

Per assegnare indirizzi IP *dinamici* agli host di una rete si può impiegare un **DHCP** (**Dynamic Host Configuration Protocol**) **server**.

Quando un host si connette inizialmente alla rete, invia in broadcast una richiesta DHCP (nella quale l'indirizzo IP sorgente è impostato a 0.0.0.0, poiché il mittente non ha ancora un indirizzo). Se nella rete è presente un DHCP server, questo risponde assegnando all'host uno degli indirizzi disponibili.

Se in una stessa rete locale sono presenti più DHCP server (ad esempio per motivi di bilanciamento del carico), il server che risponde a una determinata richiesta, fornendo un indirizzo IP, è il primo ad aver ricevuto tale richiesta.

Infine, se nella rete locale non è disponibile alcun DHCP server, ma invece è presente un router opportunamente configurato, le richieste DHCP possono essere inoltrate verso un'altra rete.

Oltre che per assegnare indirizzi privati all'interno di una LAN, il DHCP può anche essere usato dagli ISP per l'assegnazione dinamica di indirizzi pubblici ai propri clienti.

6 Zero configuration networking

Un metodo alternativo per la configurazione automatica di piccole reti, in cui non è disponibile un DHCP server, è lo **zero configuration networking**. Esso fa uso di un

range di indirizzi IP **link-local**, appositamente riservati. Questi indirizzi sono di tipo privato, cioè non possono essere usati per inoltrare dati all'esterno della rete locale.

Quando una macchina si connette alla rete, estrae casualmente un indirizzi IP link-local, e manda in broadcast un messaggio di **ARP probe** (una speciale ARP request) per determinare se tale indirizzo è già in uso. Se necessario, il processo si ripete finché non viene trovato un indirizzo libero, che infine l'host assegna a se stesso, annunciando tale assegnamento con un messaggio di **ARP announcement**.