

Generalità sul protocollo IP

A cura del prof. Giuseppe Mastrandrea
Sistemi e Reti

A.S. 2019/2020

I.I.S. A. Righi - Cerignola (FG)

| | |
|--------------------------------------|----------|
| Introduzione | 2 |
| Grafi | 2 |
| Protocollo IP | 5 |
| Indirizzi IP | 5 |
| Formato del datagramma IP | 6 |
| Utility: ping e traceroute | 10 |
| Ping: round-trip time | 10 |
| Traceroute | 12 |
| Geolocalizzazione degli indirizzi IP | 13 |
| Reti pubbliche e reti private | 14 |

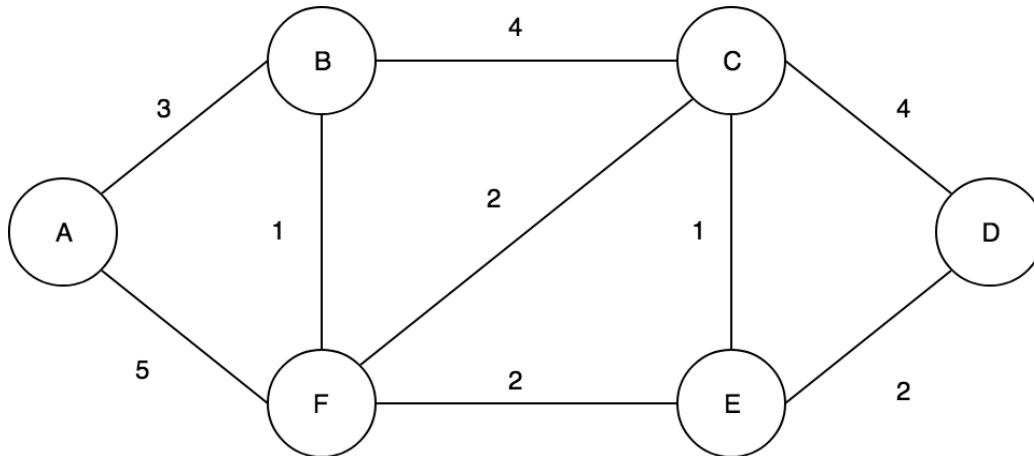
Introduzione

Una volta compreso come funziona la comunicazione tra host adiacenti, cioè host che condividono uno stesso mezzo fisico, è arrivato il turno di salire di livello e occuparci del livello di rete. Il livello di rete offre il macro-servizio di comunicazione **end-to-end**, ovvero: offre il servizio di comunicazione fra i nodi terminali di una comunicazione. Per fare questo il livello di rete sfrutta il livello sottostante (data-link), basato sulle tipologie di collegamento, per offrire un concetto di rete di computer molto più generico. A livello di rete infatti **non ci interessa più come siamo connessi ad una rete**. Un host che faccia parte di una rete a livello 3 (o rete IP, dal nome del principale protocollo di livello di rete: **Internet Protocol**) è un generico membro della rete, e prende il nome di **host**.

Grafi

Prima di parlare più nel dettaglio del livello di rete e sue funzionalità è fondamentale capire se esiste un modo rappresentare una rete in maniera generica come un insieme di host connessi fra loro. Effettivamente questo modo generico di rappresentare una rete esiste, ed è preso direttamente dalla matematica. È infatti possibile rappresentare una rete con una struttura matematica che prende il nome di **grafo**. Un grafo è la rappresentazione matematica equivalente di una rete nel networking. Dal punto di vista formale, **un grafo $G(V, E)$ è una coppia di due insiemi V e E che indicano rispettivamente un insieme di vertici o nodi (Vertices) e lati o archi (Edges)**. Meno formalmente, è possibile immaginarsi un grafo come un insieme di nodi e di archi che connettono coppie di nodi. Abbiamo svariate tipologie di grafi. In questa fase noi ci concentreremo sui grafi **connessi** (cioè un grafo in cui per ogni coppia di vertici, esiste almeno un cammino che li collega) e **pesati** (cioè grafi in cui ad ogni arco è associato un numero detto **peso**).

Gli archi di un grafo pesato hanno un numero ad essi associato che ne indica il peso (in questo caso si parla di *grafo pesato*), e che si indica con $c(x, y)$, dove x e y sono due nodi arbitrariamente scelti. Il costo per andare da un nodo ad un altro è semplicemente la somma dei pesi degli archi attraversati lungo il percorso fra i 2 nodi.



Gli insiemi che formano il grafo in figura sono:

$$V = \{A, B, C, D, E, F\}$$

$$E = \{ (A,B), (A,F), (B,C), (B,F), (C,D), (C,E), (C,F), (D,E), (E,F) \}$$

Ipotizzando il seguente percorso fra il nodo F e il nodo D:

$$F, C, E, D$$

il costo di questo percorso è semplicemente la somma dei pesi lungo gli archi attraversati:

$$c(F, C) + c(C, E) + c(E, D) = 2 + 1 + 2 = 5$$

Ritornando alle reti, ogni nodo del grafo rappresenta un host della rete e ogni arco un collegamento verso un altro host. Come avviene dunque la comunicazione fra due host di una rete IP? I messaggi che escono da un host non arrivano direttamente da un host all'altro, ma passano -appunto- attraverso gli archi della rete fino a raggiungere l'host destinazione. I costi presenti sugli archi sono dei numeri che potrebbero rappresentare caratteristiche del collegamento fra i nodi come bitrate, affidabilità, etc. Ad esempio: tramite il nostro smartphone vogliamo visitare un sito Internet. Il nostro smartphone rappresenta un nodo della rete Internet, che è una rete IP. Questo significa che il nostro smartphone può essere visto come un nodo del grafo che rappresenta la rete Internet: diciamo che rappresentiamo la rete Internet con il grafo in figura (nella realtà la rete Internet è formata da milioni di nodi interconnessi fra loro) e che il nostro smartphone sia il nodo A. Anche il sito che vogliamo visitare risiede su un computer che fa parte della rete Internet (altrimenti non potremmo visitarlo), quindi ovviamente anch'esso può essere rappresentato come un nodo di un grafo: diciamo che sia il nodo D. Quali e quanti percorsi esistono fra il nodo A e il nodo D in figura?

1. A, B, C, D
2. A, F, E, D
3. A, F, C, D
4. A, B, F, C, D
5. A, B, F, E, D
6. A, B, C, E, D
7. A, F, B, C, D
8. A, F, C, E, D
9. A, F, E, C, D
10. A, B, C, F, E, D
11. A, B, F, C, E, D

Notiamo che un percorso è valido solo se un nodo viene visitato al più una volta sola lungo la comunicazione (non possono esserci *anelli* o *circoli*). Abbiamo detto all'inizio della sezione che il livello di rete si occupa di gestire la comunicazione end to end. In questo caso quindi si occupa di gestire la comunicazione fra il nodo A (il nostro smartphone) e il nodo D (il sito che vogliamo visitare). Per garantire questo servizio, il livello di rete deve gestire quindi una cosa fondamentale: la scelta del percorso fra un nodo sorgente e un nodo destinazione. Ma la scelta di un percorso casuale non sarebbe efficiente, poichè porterebbe (ad esempio) a ritardi nella comunicazione, perdite di messaggi, e in generale problemi che renderebbero la comunicazione non ottimale. Il livello di rete non si accontenta di scegliere un percorso qualsiasi: il suo compito è quello di scegliere il percorso più adatto fra quelli disponibili. Il percorso migliore è quello a **costo minore**. Quindi nel nostro caso, il livello di rete calcola per tutti i percorsi possibili il rispettivo costo, e sceglie il percorso a costo minore:

- | | | |
|-----|------------------|-------|
| 1. | A, B, C, D | => 11 |
| 2. | A, F, E, D | => 9 |
| 3. | A, F, C, D | => 11 |
| 4. | A, B, F, C, D | => 10 |
| 5. | A, B, F, E, D | => 8 |
| 6. | A, B, C, E, D | => 10 |
| 7. | A, F, B, C, D | => 14 |
| 8. | A, F, C, E, D | => 10 |
| 9. | A, F, E, C, D | => 12 |
| 10. | A, B, C, F, E, D | => 14 |
| 11. | A, B, F, C, E, D | => 9 |

Il livello di rete sceglierà il percorso a costo minore (cioè il n. 5) per consegnare un messaggio dal nodo A al nodo D. Per trovare il percorso a costo minore il livello di rete si serve di algoritmi che siano in grado di trovare il percorso a costo minimo e di protocolli di routing.

Questa importantissima funzionalità del livello di rete prende il nome di **routing** o **instradamento**. Esso è un servizio **esterno** o **globale**, ovvero fornito dal livello di rete nella sua globalità. L'altra funzionalità tramite la quale il livello di rete offre il servizio di

comunicazione end to end è il **forwarding** o **inoltrare**: strettamente connesso al routing, esso consiste nella capacità degli host, in base alle informazioni ricavate dai protocolli di routing, di inoltrare un determinato messaggio sull'arco appropriato. Ad esempio, nel percorso 5, il nodo F utilizza il forwarding per fare viaggiare il messaggio sull'arco appropriato: in questo caso il nodo F fa viaggiare il messaggio sull'arco (F, E), perchè sa che il percorso migliore (quello selezionato dal livello di rete grazie al routing) è il percorso A, B, F, E, D. Il forwarding è un servizio **interno** ai nodi che compongono una rete IP.

Protocollo IP

Ma al di là delle strutture matematiche, quali sono le regole di Internet? Ovviamente il traffico Internet è regolato da regole molto rigide. A livello di rete, il protocollo più importante e senza il quale Internet stessa non esisterebbe è il **protocollo IP** (Internet Protocol, RFC 791). IP è un insieme molto complesso di regole e formati di scambio di dati. In questa fase ci limiteremo ad esaminare le sue caratteristiche peculiari senza scendere troppo nel dettaglio.

Indirizzi IP

Abbiamo già introdotto il concetto di "indirizzo" analizzando il livello data-link. Il concetto di indirizzo a livello di rete (d'ora in poi **indirizzo di rete** o **indirizzo logico** o **indirizzo IP**) presenta alcuni aspetti comuni con quello di indirizzo a livello data-link. Un indirizzo di livello data-link è noto solo ai dispositivi fra loro contigui, mentre un indirizzo di rete, potenzialmente, è universalmente conosciuto. L'indirizzo IP è associato al singolo dispositivo connesso ad una rete IP. Per cercare un parallelo, prendiamo ad esempio la posta tradizionale. Per far arrivare una lettera a destinazione c'è bisogno di scrivere sulla busta: nazione, città, CAP, via e numero civico. Tutte queste singole informazioni formano l'indirizzo. Esso è strettamente dipendente dal luogo fisico in cui si trova un destinatario: due nazioni diverse hanno due indirizzi diversi. Se ci trasferiamo da una nazione all'altra avremo indirizzi diversi: allo stesso modo, se un dispositivo si muove da una porzione di Internet ad un'altra, esso cambierà indirizzo IP. Che cosa intendiamo per "porzione"? Come vengono assegnati gli indirizzi IP? Per rispondere a queste domande dobbiamo capire come è strutturata la rete Internet. Essa è fatta da una serie di sistemi autonomi (cioè da gruppi di computer, cioè da grafi) gestiti da una serie di aziende chiamate **ISP (Internet Service Provider)**. I provider del servizio Internet in sostanza gestiscono quindi delle porzioni di Internet rappresentate da grafi. Cosa intendiamo per "gestire"? Fra le altre cose, essi (i provider) forniscono i loro clienti di indirizzi IP, quindi sostanzialmente fanno in modo che un loro cliente faccia parte del grafo, cioè della rete Internet, e quindi possano raggiungere ed essere raggiunti da un qualsiasi altro nodo presente sulla rete Internet. Un aspetto molto importante legato all'assegnazione degli indirizzi IP è il seguente: **in una rete IP, non possono esserci due host che abbiano lo stesso indirizzo IP**. Sarebbe come dire che 2 persone completamente diverse avessero lo stesso indirizzo: il servizio postale non saprebbe a chi consegnare la posta destinata a quell'indirizzo! Detto questo, cerchiamo di capire come è fatto un indirizzo IP.

Un indirizzo IP è lungo 4 byte (32 bit). Per rappresentarlo in una forma più human readable, ogni byte viene convertito in un numero decimale e viene separato dagli altri byte da un punto:

00001010 01111011 00001100 00000001

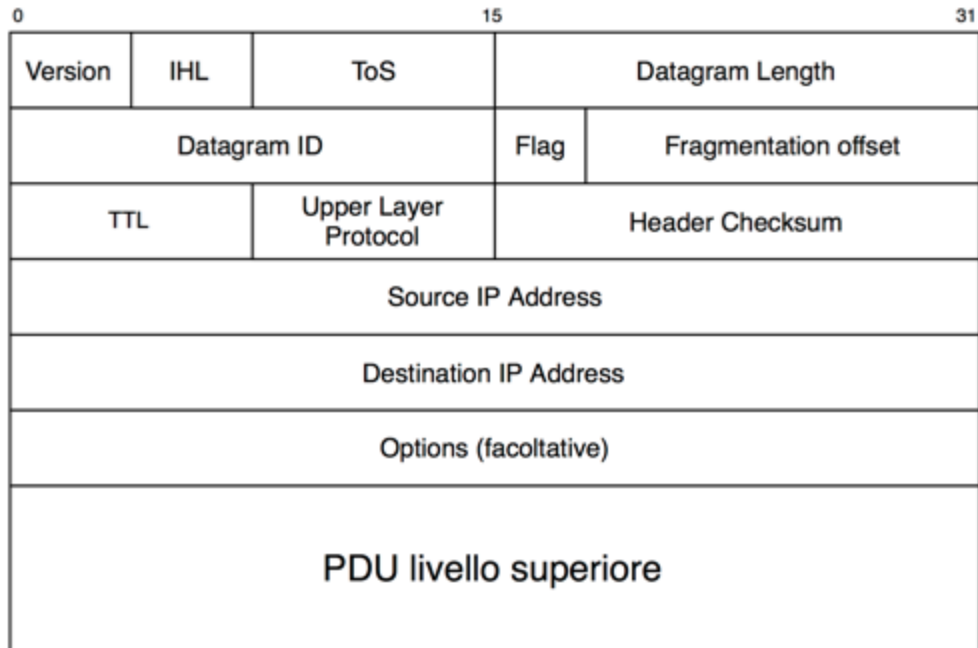
10.123.12.1

Un indirizzo IP rappresenta semplicemente un modo per raggiungere un host all'interno di una rete IP. Essendo Internet una rete IP (che connette centinaia di milioni di nodi sparsi in tutto il mondo fra loro), possiamo dire che un indirizzo IP rappresenta l'indirizzo di un nodo della rete Internet, ovvero **rappresenta l'indirizzo di un qualsiasi host connesso ad Internet**. Pensiamo ad un sito internet (Facebook, Instagram, i siti dei quotidiani), ad un servizio di streaming (Youtube, Spotify, Netflix), ad un servizio di Instant Messaging (Skype, Whatsapp, Telegram). Tutte queste piattaforme "fanno parte" di Internet: cioè esse sono raggiungibili via Internet. Ma internet è una rete IP. Quindi, esse si trovano su un computer che ha un indirizzo IP nella rete Internet, vale a dire su un **host**. Quando un utente generico si connette ad un sito Internet, o usa uno di questi servizi di streaming o di IM, in realtà egli si sta connettendo ad un computer con un determinato indirizzo IP.

Come avviene dunque la comunicazione via Internet? Dalle nostre nozioni sull'incapsulamento, sappiamo che a livello di rete viene costruita una PDU contenente un certo tipo di informazioni. Sappiamo inoltre che il livello di rete si occupa della comunicazione end to end (cioè fra gli host terminali). Alla luce di queste nozioni, è abbastanza immediato immaginare il contenuto principale di una PDU di livello di rete: essa contiene principalmente gli **indirizzi IP sorgente e destinazione** per una determinata comunicazione.

Formato del datagramma IP

Abbiamo visto i campi più importanti della PDU di livello di rete (che, a proposito, prende il nome di **datagramma IP**), vale a dire gli indirizzi IP sorgente e destinazione. Ma quali informazioni contengono gli altri campi del datagramma?



Come al solito, il datagramma IP (cioè la PDU di livello di rete) contiene un **header** e dei **dati**. In figura l'header è formato dai campi che sono aggiunti dalla fase di imbustamento del protocollo IP, mentre i dati sono rappresentati dal campo "PDU di livello superiore". Di seguito la descrizione di alcuni dei campi notevoli.

Version (4 bit): numero di versione del protocollo IP. Solitamente è uguale a 4 o 6 (ipv4 o ipv6) ma può avere altri valori che specificano formati diversi per il datagram.

IHL (4 bit): **Internet Header Length**; siccome un datagram può contenere un numero variabile di opzioni (campo options nella figura), è necessario avere un campo dedicato alla lunghezza della sola intestazione IP: è proprio il campo IHL. Quindi il campo **IHL ci dice la lunghezza della parte "header" di un datagramma IP**. Per ottenere il valore in byte dell'header bisogna moltiplicare per 4 il valore contenuto nel campo IHL:

Ad esempio, se nel campo IHL è contenuto il valore in bit 0101, per ottenere la dimensione dell'header in byte dovremo convertire il numero in decimale e moltiplicare quel valore per 4:

$$(0101)_2 = (5)_{10} = 5 * 4 = 20 \text{ byte}$$

ToS (8 bit): **Type of Service**: serve a distinguere diversi servizi richiesti dai protocolli superiori (es. jitter limitato, consegna garantita). I primi 3 bit servono a settare la priorità. Non sono usati al giorno d'oggi. Gli altro 4 bit sono detti di servizio e alcuni valori notevoli sono:

- 0000: traffico normale
- 0001: minimizzare il costo
- 0010: massimizza affidabilità
- 0100: massimizza throughput
- 1000: minimizza delay

Total length (16 bit): Indica la lunghezza di tutta la PDU di livello 3 (header + PDU livello superiore). Essendo il campo da 16 bit, ne consegue che la grandezza massima di un datagramma IP (header + dati) è di 65535 byte.

Datagram ID, flag, fragmentation offset (32 bit): Hanno a che fare con la frammentazione IP (trattata più avanti). Non presenti in IPv6

TTL (Time To Live – 8 bit): Costituisce il tempo di vita in secondi prima che il datagramma in esame sia scartato. È decrementato di 1 ogni volta che un datagram transita attraverso un nodo intermedio (router). Valori alti possono significare varie cose:

- Rete lenta
- Traffico non critico

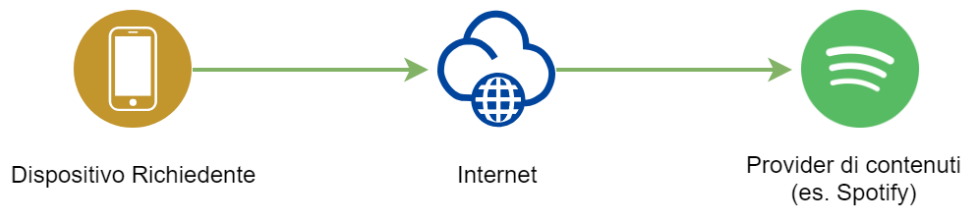
Upper Layer Protocol (8 bit): Usato quando il campo raggiunge la destinazione finale. Indica il protocollo a livello di trasporto (quindi di livello superiore) utilizzato.

Internet checksum (16 bit): Rappresenta il checksum della sola intestazione, non anche dei dati. Si calcola con le regole già viste per il livello data-link.

Source/Destination address (32 bit ciascuno): si tratta degli indirizzi IP sorgente e destinazione. Non cambiano lungo il percorso, vengono rimbalzati da un nodo all'altro del grafo che rappresenta la rete in base ai protocolli e agli algoritmi di routing.

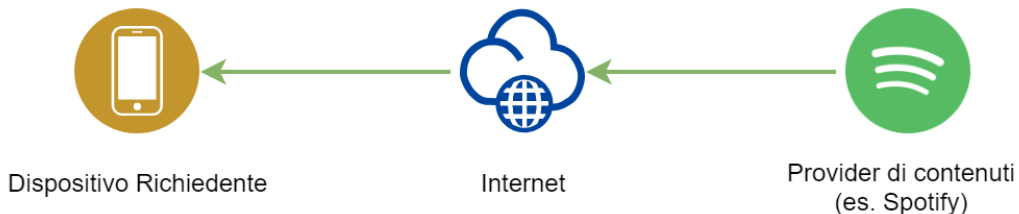
Ma qual è il senso di questa PDU? A che serve? Come funziona il protocollo IP? Pensiamo ad una busta contenente un messaggio di posta tradizionale: essa contiene l'indirizzo del destinatario della nostra lettera sul retro, mentre davanti contiene (o perlomeno è buona norma che contenga) l'indirizzo del mittente della lettera, in maniera che il destinatario della nostra lettera non solo sappia chi gli ha scritto, ma possa anche spedire ad un preciso indirizzo un'eventuale risposta alla lettera. Trasportando questo esempio alla rete Internet, quando proviamo a connetterci ad un sito Internet, o proviamo ad ascoltare una canzone o vedere un film utilizzando un servizio di streaming (es. Spotify, Netflix, Youtube), fondamentalmente stiamo applicando lo stesso principio della posta tradizionale: dal nostro dispositivo esce un messaggio indirizzato verso il nodo della rete Internet (cioè l'host) contenente le informazioni che cerchiamo; siccome fa parte della rete Internet, esso ha un indirizzo IP. Ma anche il nostro dispositivo fa parte della rete Internet, e anch'esso quindi è dotato di un indirizzo IP. Succede quindi che dal nostro dispositivo parte un messaggio che a livello di rete contiene *l'indirizzo IP del nostro dispositivo* come indirizzo sorgente (mittente) e *l'indirizzo IP della piattaforma da cui vogliamo informazioni* (destinatario) come indirizzo destinazione. La nostra richiesta viaggia attraverso il grafo che rappresenta la rete Internet e viene recapitata a destinazione (il nodo della rete IP corrispondente al sito Internet o alla piattaforma da cui vogliamo dei contenuti).

Richiesta: "Fammi ascoltare una canzone"



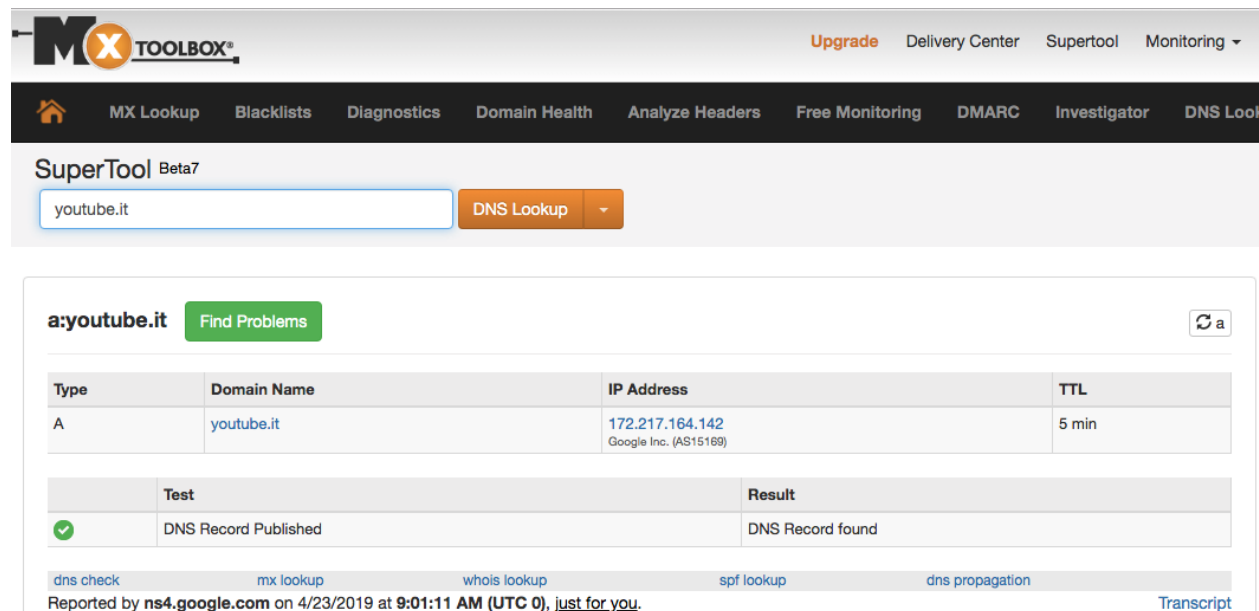
Come è possibile che quei dati poi ritornino indietro? Facile: nella richiesta partita dal nostro dispositivo viene specificato anche l'indirizzo IP sorgente, quindi il provider di contenuti non farà altro che spedire indietro sulla rete Internet un altro messaggio contenente i dati che erano stati richiesti, stavolta con gli indirizzi scambiati:

Risposta: "Certo! Eccoti la canzone"



Sorge quindi spontanea una domanda: come è possibile conoscere l'indirizzo IP di un fornitore di servizi (nel nostro esempio Spotify)? Per un essere umano è più facile ricordarsi un nome di dominio (es. facebook.com, instagram.com, youtube.it, ilpost.it, etc) che una serie di numeri. Per questo è stato inventato il protocollo **DNS** (Domain Name System), che si occupa di

effettuare la conversione da un nome di dominio ad un indirizzo IP. In questo modo un utente piuttosto che connettersi ad un sito utilizzando il suo indirizzo IP, può digitare il nome associato a quell'indirizzo e lasciare che sia il protocollo DNS a effettuare la conversione. Chiunque sia curioso di scoprire quale sia l'indirizzo IP corrispondente ad un determinato sito Internet può usare uno degli innumerevoli strumenti presenti online, per esempio il SuperTool di MxToolbox.



The screenshot shows the MxToolbox SuperTool interface. At the top, there is a navigation bar with the MxToolbox logo and links for Upgrade, Delivery Center, Supertool, and Monitoring. Below this is a secondary navigation bar with links for MX Lookup, Blacklists, Diagnostics, Domain Health, Analyze Headers, Free Monitoring, DMARC, Investigator, and DNS Look. The main content area is titled "SuperTool Beta7" and features a search input field containing "youtube.it" and a "DNS Lookup" button. Below the search bar, there is a section for "a:youtube.it" with a "Find Problems" button and a refresh icon. A table displays the DNS lookup results:

| Type | Domain Name | IP Address | TTL |
|------|-------------|--|-------|
| A | youtube.it | 172.217.164.142 Google Inc. (AS15169) | 5 min |

Below the table, there is a "Test" section with a table showing the result of the DNS lookup:

| Test | Result |
|------------------------|------------------|
| ✓ DNS Record Published | DNS Record found |

At the bottom, there are links for "dns check", "mx lookup", "whois lookup", "spf lookup", and "dns propagation". A footer note states: "Reported by ns4.google.com on 4/23/2019 at 9:01:11 AM (UTC 0), just for you." and a "Transcript" link.

Al contrario, come è possibile conoscere l'indirizzo IP del *proprio* dispositivo? Anche per risolvere questo problema esiste una moltitudine di siti Internet specializzati. Uno fra i più conosciuti è <https://www.whatsmyip.org/>.

A decidere come effettuare la "distribuzione" degli indirizzi IP è l'ISP che ci fornisce la connessione (Tim, Vodafone, Wind, Tre, etc.). Se un indirizzo IP viene assegnato in maniera permanente ad un utente si parla di **indirizzamento fisso** (Fastweb è un ISP che fornisce indirizzamento fisso), mentre se gli indirizzi IP variano ogni volta che ci connettiamo/disconnettiamo dalla rete dati si parla di **indirizzamento dinamico**.

Utility: ping e traceroute

Ping: round-trip time

Un'alternativa per scoprire un indirizzo IP di un host, e anche per avere altre informazioni, è un software chiamato "**ping**", e presente in tutti i sistemi operativi. Ping è in realtà un programma che serve a capire quanto tempo ci impiega un pacchetto di dati di una certa dimensione a raggiungere un certo host su Internet; ci fornisce quindi informazioni relative al tempo di connessione verso un certo host. Minore sarà il tempo, ovviamente, migliore sarà la qualità della connessione verso quell'host. Per aprirlo da Windows basta:

- Su windows, premere la combinazione di tasti “Win” + “R” (apre la finestra di dialogo “esegui”) oppure su un sistema operativo Linux o Mac OS aprire “terminale”
- Solo Windows: digitare “cmd” e premere invio (apre il prompt dei comandi di windows, un’interfaccia a caratteri per usare windows)
- Nella finestra di dialogo che si aprirà digitare “ping *nomedominio*”

L’output di questa serie di passaggi sarà qualcosa di simile a questo (screenshot di un comando ping eseguito da un sistema operativo Mac OS):

```
Mac-mini-di-Mac:~ giumast$ ping youtube.it
PING youtube.it (172.217.23.110): 56 data bytes
64 bytes from 172.217.23.110: icmp_seq=0 ttl=54 time=94.798 ms
64 bytes from 172.217.23.110: icmp_seq=1 ttl=54 time=88.682 ms
64 bytes from 172.217.23.110: icmp_seq=2 ttl=54 time=70.623 ms
64 bytes from 172.217.23.110: icmp_seq=3 ttl=54 time=38.267 ms
^C
--- youtube.it ping statistics ---
4 packets transmitted, 4 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 38.267/73.093/94.798/21.983 ms
```

Analizziamo l’output che ci è restituito dal comando “ping”:

- Alla prima riga vediamo la corrispondenza nome di dominio/indirizzo IP. Il programma ci informa che sta effettuando un ping verso youtube.it, che ha indirizzo IP pari a 172.217.23.110, utilizzando dei pacchetti di dati grandi 56 byte.
- Le 4 righe successive ci dicono invece che abbiamo provato a mandare 4 pacchetti di dati e che l’host 172.217.23.110 ci ha risposto con pacchetti di dati grandi 64 byte, mandati nell’ordine indicato dal numero “icmp_seq” (0,1,2,3) in un tempo rispettivamente pari a: 94.798 millisecondi, 88.682 millisecondi, 70.623 millisecondi, 38.267millisecondi.
- Infine nelle ultime due righe troviamo le statistiche:
 - 4 pacchetti di dati inviati
 - 4 pacchetti di risposta ricevuti
 - Percentuale di pacchetti persi: 0.0% (tutti i pacchetti inviati sono ritornati indietro)
- Infine abbiamo informazioni sul tempo di *round-trip*, cioè il tempo che è trascorso da quando abbiamo inviato il messaggio di test fino al momento in cui è tornato indietro il messaggio:
 - Round Trip minimo
 - Round trip medio
 - Round trip massimo

- Deviazione standard

Traceroute

Un'altra utility molto importante per comprendere a fondo cosa succede quando ci connettiamo ad un certo host su internet è **traceroute** (su Windows abbreviato in **tracert**). Nella parte introduttiva sul livello di rete abbiamo infatti detto che il livello di rete gestisce la comunicazione end to end, cioè fra nodi terminali. Quello che accade però è che il pacchetto di dati (richieste e risposte) viaggiano nel grafo che è Internet, ovvero vengono inoltrati di nodo in nodo fino a raggiungere il nodo di destinazione. L'utility traceroute ci indica esattamente quale percorso fa all'interno del grafo che rappresenta Internet un certo pacchetto di dati prima di raggiungere una destinazione che noi specifichiamo. Per usare traceroute basta effettuare i seguenti passaggi:

- Su windows, premere la combinazione di tasti "Win" + "R" (apre la finestra di dialogo "esegui") oppure su un sistema operativo Linux o Mac OS aprire "terminale";
- Solo Windows: digitare "cmd" e premere invio (apre il prompt dei comandi di windows, un'interfaccia a caratteri per usare windows);
- Nella finestra di dialogo che si aprirà digitare "tracert *nomedominio*" (su windows) o "traceroute *nomedominio*" su Mac OS o Linux

L'output di questa serie di passaggi sarà qualcosa di simile a questo (screenshot di un comando traceroute eseguito da un sistema operativo Mac OS):

```
Mac-mini-di-Mac:~ giuamast$ traceroute youtube.it
traceroute to youtube.it (216.58.205.78), 64 hops max, 52 byte packets
 1  modemtim (192.168.1.1)  36.246 ms  2.133 ms  11.455 ms
 2  * * *
 3  172.17.144.214 (172.17.144.214)  33.690 ms
    172.17.144.212 (172.17.144.212)  28.541 ms
    172.17.144.250 (172.17.144.250)  58.707 ms
 4  172.17.145.108 (172.17.145.108)  62.256 ms
    172.17.145.126 (172.17.145.126)  93.316 ms
    172.17.145.116 (172.17.145.116)  7.209 ms
 5  172.19.245.81 (172.19.245.81)  76.652 ms
    172.19.245.77 (172.19.245.77)  54.703 ms  106.236 ms
 6  etrunk12.milano1.mil.seabone.net (93.186.128.205)  60.008 ms
    etrunk38.milano50.mil.seabone.net (195.22.196.92)  92.532 ms
    etrunk12.milano1.mil.seabone.net (93.186.128.205)  39.871 ms
 7  74.125.51.148 (74.125.51.148)  87.122 ms
    72.14.195.206 (72.14.195.206)  98.883 ms
    72.14.204.72 (72.14.204.72)  106.280 ms
 8  108.170.245.65 (108.170.245.65)  62.555 ms
    108.170.245.81 (108.170.245.81)  63.045 ms
    108.170.245.65 (108.170.245.65)  55.317 ms
 9  216.239.42.11 (216.239.42.11)  88.721 ms * 116.771 ms
10  mil04s25-in-f14.1e100.net (216.58.205.78)  95.008 ms  91.958 ms  93.159 ms
```

Semplificando di molto, potremmo dire che il comando traceroute manda 3 pacchetti di dati verso l'host destinazione (in questo caso 216.58.205.78) e "registra" ogni passaggio, vale

a dire l'indirizzo IP di ogni nodo intermedio del grafo prima di raggiungere il nodo host di destinazione finale (il server di youtube.it), specificando anche il round trip time (analogamente a quanto fa ping) di ogni nodo intermedio. Notiamo che ognuno dei 3 pacchetti può fare percorsi diversi (motivo per cui per i passaggi 3, 4, 7, 8) abbiamo 3 indirizzi IP diversi, mentre per il passaggio 5 ne abbiamo 2. Notiamo anche che nel passaggio 2 abbiamo degli asterischi, che indicano una perdita di dati. In questo caso traceroute cercherà un altro percorso per arrivare a destinazione.

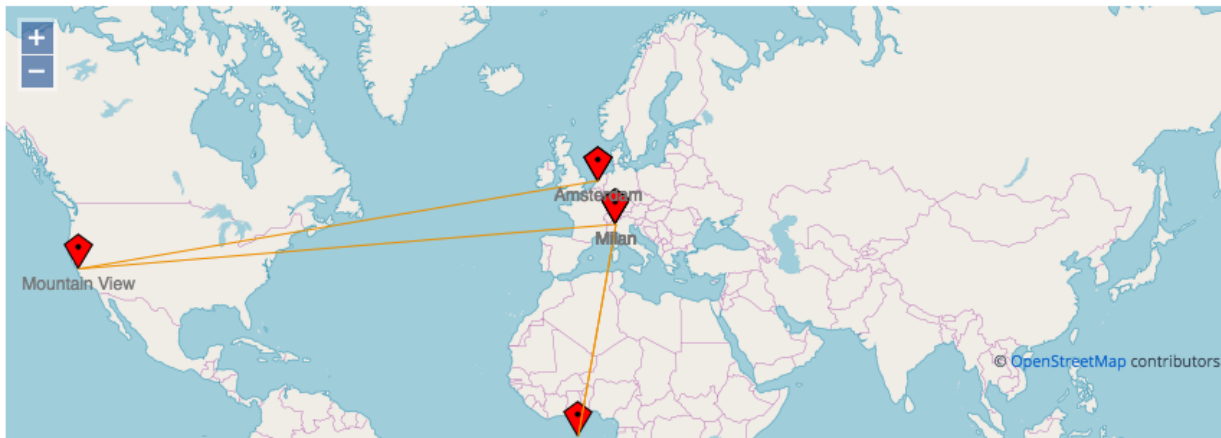
Geolocalizzazione degli indirizzi IP

Finora abbiamo parlato solo di indirizzi IP e di host. Ma se è vero che questi host sono dei nodi della rete, è anche vero che essi si troveranno da qualche parte nel mondo. I servizi di geolocalizzazione servono proprio a risalire ad una locazione fisica (intesa come coordinate geografiche di latitudine e longitudine) di un nodo della rete Internet con un certo indirizzo IP. Ce ne sono di gratuiti (meno accurati) e a pagamento, di solito molto accurati. In realtà gli unici a poter fornire informazioni molto dettagliate sulle coordinate geografiche di un certo indirizzo IP sono i fornitori di servizi Internet (ISP). Ad ogni modo esistono molti servizi in grado di fornire un'indicazione di massima delle coordinate GPS di un certo indirizzo IP. La conversione da indirizzo IP a coordinate geografiche si chiama **IP lookup**. Una piattaforma molto popolare che offre il servizio di IP lookup è "Whatismyipaddress", raggiungibile all'URL <https://whatismyipaddress.com/ip-lookup>.

Lo step successivo è quello di visualizzare su una mappa tutti i passaggi dei pacchetti che transitano in una sessione traceroute. È esattamente quello che fa la piattaforma "ip2location", disponibile a questo URL: <https://www.ip2location.com/free/traceroute>

Ecco un esempio di output:

Traceroute to 216.58.205.78 from 🇮🇹 Italy



| Hop | IP Address | Hostname | Location | Time |
|-----|----------------|---------------------------|---|-------------|
| 1 | 149.154.157.1 | gw.it.milano.edis.at | 🇮🇹 Italy, Lombardia, Milan | 0.907 ms |
| 2 | 178.249.188.2 | 178.249.188.2 | 🇮🇹 Italy, Lombardia, Milan | 0.476 ms |
| 3 | 10.130.1.41 | 10.130.1.41 | LOCAL PRIVATE LAN | 2136.737 ms |
| 4 | 217.171.32.170 | 217.171.32.170 | 🇮🇹 Italy, Lombardia, Milan | 0.578 ms |
| 5 | 217.29.66.96 | google.mix-it.net | 🇮🇹 Italy, Lombardia, Milan | 0.688 ms |
| 6 | 108.170.245.81 | 108.170.245.81 | 🇺🇸 United States, California, Mountain View | 2.062 ms |
| 7 | 216.239.42.11 | 216.239.42.11 | 🇳🇱 Netherlands, Noord-Holland, Amsterdam | 0.595 ms |
| 8 | 216.58.205.78 | mil04s25-in-f78.1e100.net | 🇳🇱 Netherlands, Noord-Holland, Amsterdam | 0.535 ms |

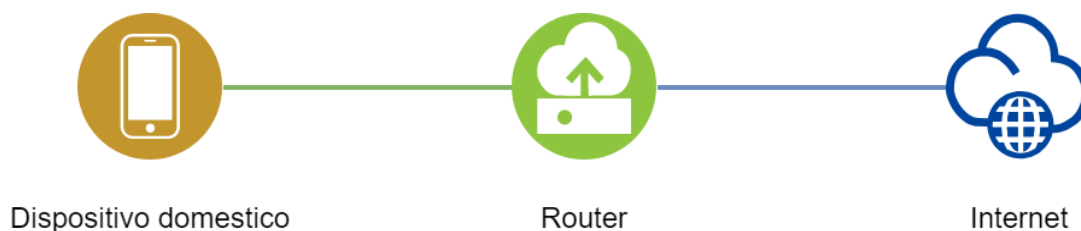
Reti pubbliche e reti private

Nella figura precedente, oltre ai normali passaggi attraverso nodi del grafo che rappresenta Internet, c'è una riga che ancora non siamo in grado di interpretare. La riga 3 infatti è contrassegnata dalla Location "Local Private LAN". Che significa? Perché il servizio di ip lookup non è stato in grado di dirci da che nazione proviene quell'indirizzo IP?

Per rispondere a queste domande dobbiamo fare un piccolo passo indietro e tornare alla struttura generale degli indirizzi IP. Abbiamo detto che un indirizzo IP è formato da 4 byte, vale a dire 32 bit. Il che ci porta a dire che in totale ci sono 2^{32} indirizzi IP. Ma dalle nostre nozioni sulla rete Internet, dovrebbe ormai apparire chiaro che in Internet non possono esserci contemporaneamente 2 host che hanno lo stesso indirizzo IP (sarebbe come dire che persone completamente diverse fra loro hanno lo stesso indirizzo di posta, si creerebbe un'ambiguità per cui il postino non saprebbe a chi consegnare una lettera o una cartolina). Unendo queste 2 considerazioni, possiamo dedurre che in Internet non possono esserci più di 2^{32} persone connesse contemporaneamente; se così fosse tutti gli indirizzi IP sarebbero occupati e non sarebbe possibile più per nessuno ottenere un indirizzo IP univoco!

Per fronteggiare questo problema, l'IEEE ha escogitato 2 sistemi. Il primo consiste semplicemente nell'aumentare la dimensione degli indirizzi IP a 16 byte. La versione del protocollo IP che usa 16 byte si chiama **IPv6** mentre quella "tradizionale" a 4 byte si chiama **IPv4**. Tuttavia, il cambiamento di versione del protocollo non è di facile attuazione, visto che tutti gli apparati del mondo (milioni e milioni di apparati) sono stati progettati e costruiti per funzionare con IPv4. Siccome le due versioni del protocollo non sono *interoperabili* (cioè non possono funzionare insieme sullo stesso apparato) bisognerebbe sostituire o aggiornare tutti i dispositivi che fanno uso di IPv4, un'impresa titanica! Nell'attesa che questa transizione avvenga l'IEEE ha inventato un sistema più ingegnoso e compatibile al 100% con tutti gli apparati attualmente utilizzati in Internet. Questo sistema prevede la suddivisione delle reti che fanno parte di Internet in 2 grandi categorie: le **reti private** e le **reti pubbliche**.

Per capire meglio la differenza fra queste 2 reti, pensiamo alle nostre reti domestiche. Quando ci troviamo a casa e ci connettiamo con un dispositivo (un portatile, un pc fisso, una smart TV, uno smartphone) al WiFi di casa o tramite cavo Ethernet, quello che stiamo facendo è entrare a far parte della rete di casa nostra. Tutti i dispositivi che si connettono ad Internet tramite la nostra rete fanno parte della **rete privata** di casa nostra. Qual è il punto di accesso ad Internet, se utilizziamo il WiFi? Il **router**, a sua volta collegato alla rete Internet grazie ad un certo ISP (Tim, Wind, 3, Vodafone, Linkem). Il collegamento ad Internet può avvenire tramite cavo telefonico, fibra ottica, WiMAX (es. Linkem, Vodafone Station). Il collegamento al router, invece, avviene tramite WiFi o cavo Ethernet. Distinguiamo quindi 2 tipi di "connessione": la connessione fra il nostro dispositivo e il router e la connessione fra il router e la rete Internet, come illustrato nella figura successiva:



Ovviamente quando ci allontaniamo dalla portata del nostro WiFi o stacciamo il cavo Ethernet non sfruttiamo più il router per andare su Internet, vale a dire per connetterci ad un qualsiasi sito Internet o utilizzare un qualsiasi servizio di rete (messaggistica, posta elettronica, streaming, etc). Possiamo quindi dire che il router si pone come "cancello di accesso" fra i dispositivi connessi alla nostra rete domestica. Proprio per questo motivo un router che funziona in questo modo viene chiamato anche **gateway**.

In questo scenario, quando dobbiamo connetterci ad un provider di contenuti su Internet non ci connettiamo più "direttamente" ad esso (come abbiamo visto poche pagine fa), ma usiamo il nostro router come intermediario. La comunicazione avviene in questi passaggi:

1. Richiesta dal dispositivo al router: "Chiedi a Spotify di farmi ascoltare una canzone"
2. Richiesta dal router a Spotify: "Fammi ascoltare una canzone"

3. Risposta di Spotify destinata al router: “Ecco la tua canzone”
4. Risposta del router al dispositivo: “Ecco la risposta che mi ha mandato Spotify”

Come ben sappiamo anche un altro dispositivo potrebbe connettersi al router e fare la stessa richiesta. Il router è in grado di capire da chi proviene la richiesta e, una volta ricevuta la risposta da parte del provider di contenuti, inoltrare la risposta al dispositivo corretto. Il provider di contenuti, dal canto suo, non sarà mai in grado di vedere da chi proviene realmente la richiesta. Esso semplicemente dialogherà con il router, completamente ignaro del fatto che “alle spalle” di quel router ci sono i dispositivi che hanno realmente fatto le richieste.

Possiamo identificare quindi due grandi sezioni interconnesse fra loro tramite il router. La rete domestica si dice **rete privata**, mentre la rete Internet si dice **rete pubblica**. Entrambe le reti funzionano secondo il protocollo IP: questo significa che *in entrambe le reti tutti gli host hanno un indirizzo IP*. Ma che differenza c'è fra le 2 reti?

In una rete privata, gli host sono liberi di comunicare fra loro esattamente come avviene su Internet. Essa è tuttavia una rete locale (**LAN - Local Area Network**), nel senso che è formata da pochi host (se confrontata ai miliardi di host che compongono la rete Internet). Le reti private hanno a disposizione dei gruppi particolari di indirizzi IP. In particolare gli indirizzi IP appartenenti agli host di ciascuna rete possono appartenere ad una di queste 3 classi, a seconda della dimensione della rete privata:

- A. Da 10.0.0.0 a 10.255.255.255 (consente di avere reti private con più di 16 milioni di host)
- B. Da 172.16.0.0 a 172.31.255.255 (consente di avere reti private con poco più di 1 milione di host)
- C. Da 192.168.0.0 a 192.168.255.255 (consente di avere reti private con al massimo 65536 host)

Per scoprire qual è l'indirizzo IP privato del nostro computer possiamo effettuare i seguenti passaggi:

- Su windows, premere la combinazione di tasti “Win” + “R” (apre la finestra di dialogo “esegui”) oppure su un sistema operativo Linux o Mac OS aprire “terminale”;
- Solo Windows: digitare “cmd” e premere invio (apre il prompt dei comandi di windows, un'interfaccia a caratteri per usare windows);
- Nella finestra di dialogo che si aprirà digitare “ipconfig” (su windows) o “ifconfig” su Mac OS o Linux

Fra le informazioni che ci appariranno a schermo, dovremo cercare il tipo di connessione che stiamo utilizzando per comunicare con il router (WiFi, Ethernet, Bluetooth, etc) e cercare la dicitura “Indirizzo IPv4”:

```
C:\Users\Chalie>ipconfig

Configurazione IP di Windows

Scheda LAN wireless Connessione alla rete locale (LAN)* 2:

    Stato supporto. . . . . : Supporto disconnesso
    Suffisso DNS specifico per connessione:

Scheda LAN wireless Connessione alla rete locale (LAN)* 3:

    Stato supporto. . . . . : Supporto disconnesso
    Suffisso DNS specifico per connessione:

Scheda LAN wireless Wi-Fi:

    Suffisso DNS specifico per connessione: homenet.telecomitalia.it
    Indirizzo IPv6 locale rispetto al collegamento . : fe80::a194:35d1:676b:5565%13
    Indirizzo IPv4. . . . . : 192.168.1.227
    Subnet mask . . . . . : 255.255.255.0
    Gateway predefinito . . . . . : 192.168.1.1

Scheda Ethernet Connessione di rete Bluetooth:

    Stato supporto. . . . . : Supporto disconnesso
    Suffisso DNS specifico per connessione:
```

In questo caso, l'indirizzo IP del computer è 192.168.1.227. Come possiamo notare, con questo comando è possibile anche sapere qual è l'indirizzo IP del gateway (vale a dire del router). La regola dell'univocità dell'indirizzo IP cambia lievemente nel caso di reti private: l'indirizzo IP 192.168.1.227 non può essere utilizzato da un altro host presente nella rete domestica di cui fa parte il computer da cui è stato lanciato il comando "ipconfig". Tuttavia, in un'altra rete domestica, un altro host potrebbe tranquillamente utilizzare quell'indirizzo IP. Tutti gli host devono avere indirizzi IP diversi solo all'interno della stessa rete privata.

Tutti gli indirizzi IP che non rientrano negli intervalli A, B, C visti in precedenza, tranne alcune eccezioni, sono **indirizzi IP pubblici**. La rete pubblica coincide con la rete Internet. Il fatto che gli indirizzi IP siano pubblici implica il fatto che tutti possono conoscere un indirizzo IP pubblico, e che quindi tutti possono raggiungere in qualsiasi momento un qualsiasi host con indirizzo IP pubblico. I router domestici, fra le loro peculiarità, hanno anche quella di avere 2 indirizzi IP: uno privato, che si interfaccia con la LAN privata domestica, e uno pubblico, che si "affaccia" su Internet e che quindi è in grado di comunicare con tutti gli host connessi ad Internet, facendo da gateway agli host connessi alla rete privata locale. In figura vediamo un esempio di come è strutturata la comunicazione tra reti private e pubbliche in Internet.

PUBLIC NETWORK

