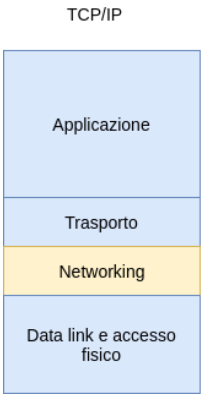
Appunti sul livello IP

Livello IP

In questo livello, i “messaggi” inviati tra gli host sono chiamati “**datagrammi IP**”



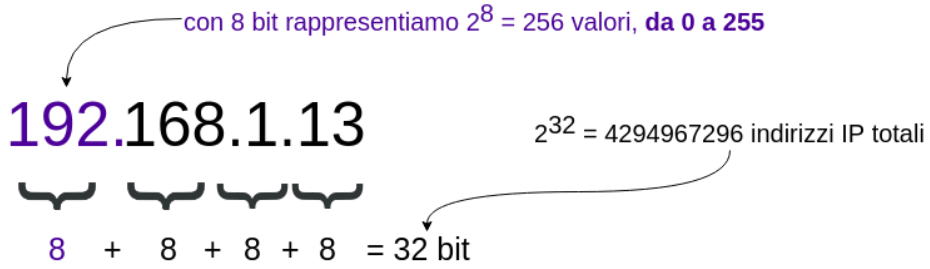
In questa parte del programma vedremo

- come vengono assegnati e gestiti gli indirizzi IP
- la distinzione tra IP pubblici e privati,
- Il problema del routing

IPv4 e IPv6

Indirizzo IP: serve ad identificare in modo esclusivo un host sulla rete Internet.

È un codice composto da **4 blocchi di numeri da 0 a 255 separati da 3 punti**,
ad esempio:



4 miliardi di indirizzi IP sembrano tanti, ma non sono tutti utilizzabili, e i dispositivi sempre connessi ad Internet sono in costante aumento.

IPv6 è un nuovo standard (non ancora in uso) che **anziché 32 bit usa 128 bit** per lo spazio di indirizzamento, permettendo 655 triliardi di indirizzi unici.

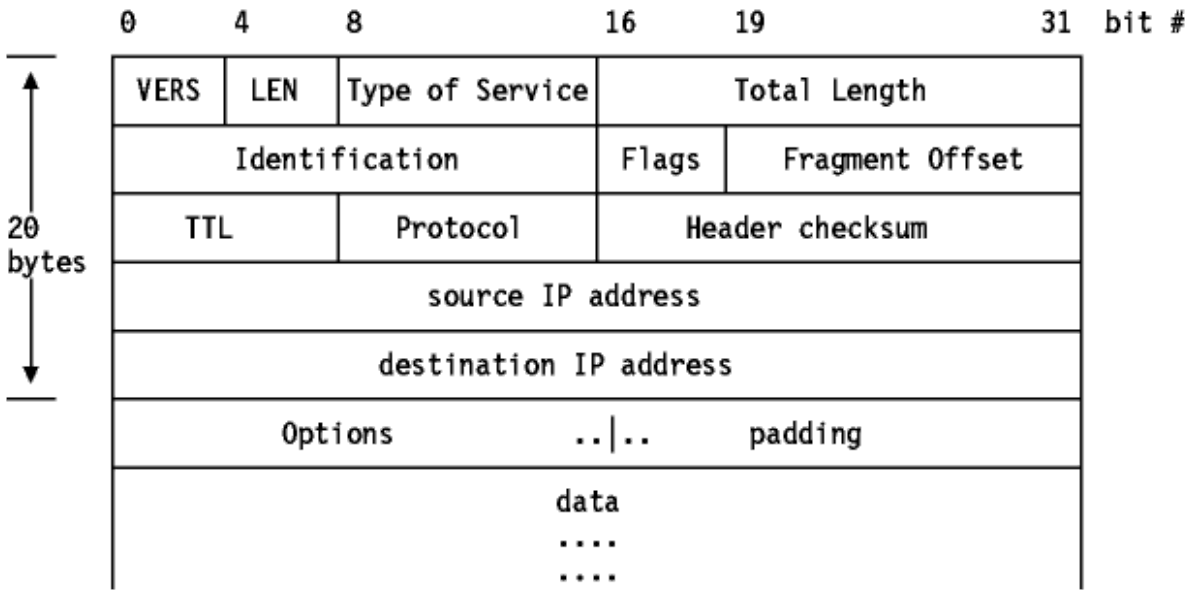
Esempio di indirizzo IPv6:

fe80:0000:0000:0000:51e1:6d16:55a:1bd

abbreviabile in

fe80::51e1:6d16:55a:1bd

Formato di un datagram IP:



Ognuno di questi campi ha un uso ben documentato, ma vediamo i più rilevanti:

- **VERS**: Versione del protocollo IP (IPv4 o IPv6)
- **LEN**: Lunghezza dell'header del datagram (in generale 5 bit (20 byte))
- **Total Length**: Lunghezza totale del datagramma IP (compreso il *payload*)
- **Identification**: Numero intero che identifica il datagram
- **TTL**: Time to Live - Viene decrementato da ciascun router per cui passa, e quando raggiunge lo zero, il datagram viene scartato (serve ad evitare cicli infiniti, vedremo)
- **Protocol**: Indica quale protocollo applicativo può usare i dati trasportati dal datagram
- **Header Checksum**: per controllare l'integrità dei dati dell'header
- **Source e Destination IP address**: IP del mittente e del destinatario
- **Data**: Anche chiamato payload, è il campo che trasporta i dati da passare al livello superiore (ricordate, incapsulamento)

Non fatevi truffare!
Come leggere la bandwidth

La metrica di prestazione utilizzata è detta “**bandwidth**” (larghezza di banda) ed indica la quantità di dati trasmessi per unità di tempo.

Ad esempio:

K**b**ps o Kbit/s → Kilo-bit per secondo
M**b**ps o Mbit/s → Mega-bit per secondo
e così via

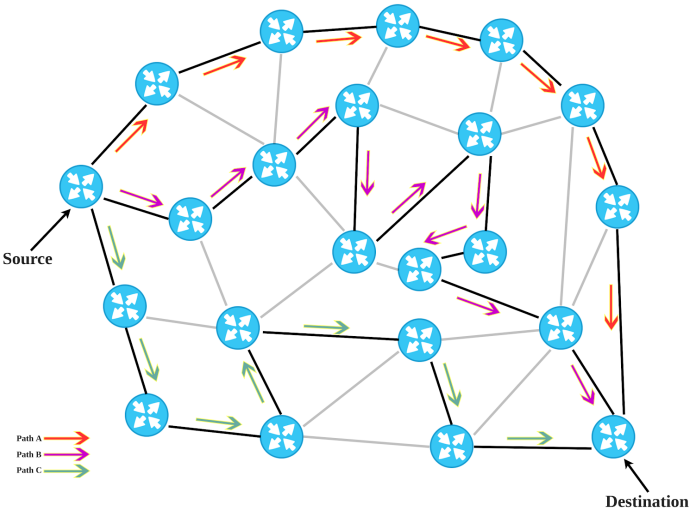
Notate la “b” minuscola, che significa **bit**.
Se avessi usato la **“B” maiuscola** avrei inteso **Byte**.

La differenza è importante perché 1 byte sono 8 bit!!!

Quando ad esempio sul vostro contratto telefonico è scritto “100 mega” è inteso **100 megabit**, ovvero 100/8 = **12,5 MB/s**. Questa è la velocità effettiva della vostra linea.

Che altro accade a livello IP

A livello IP avviene il **routing**:
⇒ Scelta del percorso di un pacchetto per arrivare da A a B (vedremo in seguito in dettaglio)



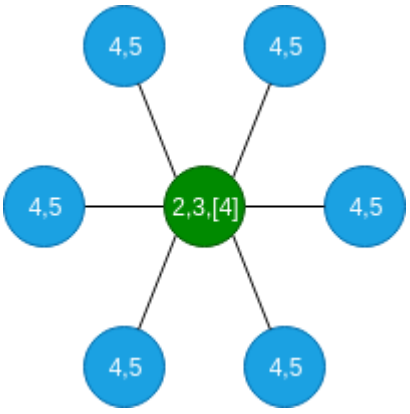
Cosa NON accade a livello IP

Il protocollo IP fornisce soltanto una **consegna non affidabile dei pacchetti:**

- La consegna è **priva di connessione** (Ogni pacchetto è trattato in modo **indipendente** da tutti gli altri, senza considerare lo storico)
- La **consegna non è garantita**: i pacchetti possono essere persi, duplicati, o arrivare fuori ordine

Perché

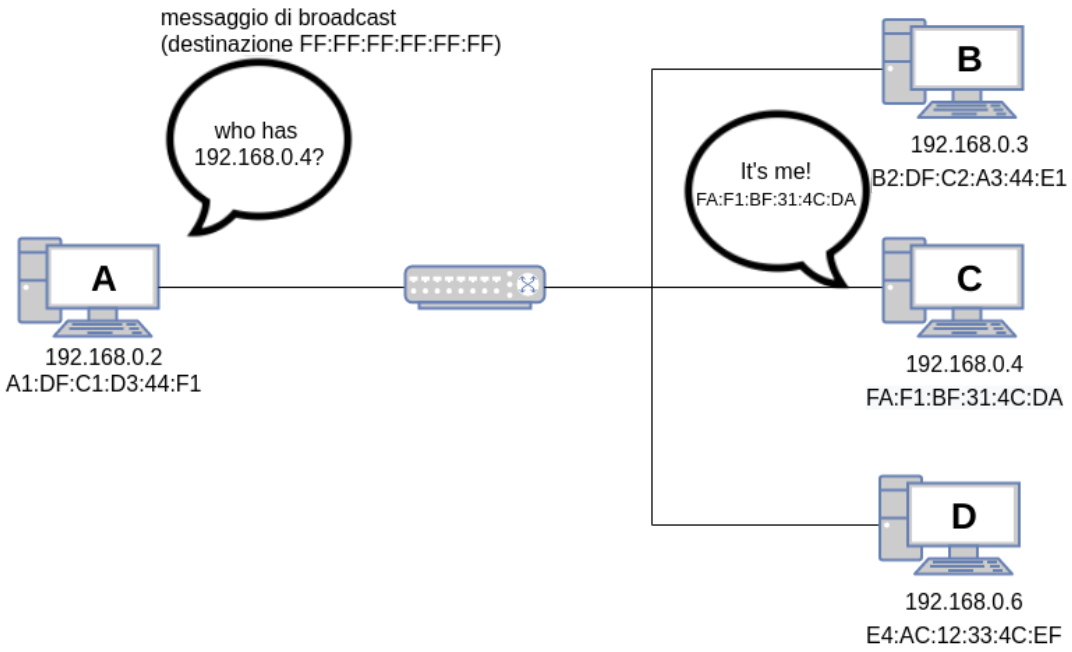
i dispositivi di livello 2 e 3 (switch e router) sono i **punti cardine della rete**: devono smistare **migliaia di pacchetti al secondo** con un hardware più possibile ridotto all'osso e avere **tempi di risposta ridotti** per non rallentare l'intera rete introducendo latenze.



<u>Il controllo di connessione e la consegna garantita sono funzionalità più avanzate</u>, che lasciamo ai protocolli di livello superiore (4 e 5) eseguiti da macchine più prestanti ai "bordi" della rete (come il PC dell'utente finale) che dovranno occuparsi solo del proprio traffico, e non smistare anche il traffico di tutti gli altri!

Il protocollo ARP

Gli host direttamente connessi alla stessa rete si identificano con il MAC Address.
Come può A mandare un messaggio all'indirizzo IP 192.168.0.4? **dovrebbe conoscere il MAC Address associato a quell'IP!**



è proprio a questo che serve il protocollo **ARP** (**A**ddress **R**esolution **P**rotocol).

Come funziona

1. **A** invia un messaggio in **broadcast** a tutti i MAC Address sulla sua rete, **chiedendo chi ha l'IP in questione**.
2. Il messaggio verrà ignorato da tutti tranne **C che risponde "sono io"**
3. A memorizza l'associazione tra IP indirizzo hardware a cui raggiungerlo.

ARP Table

L'elenco di tutte le associazioni **MAC Address : IP Address** è salvato nella "**ARP Cache**", anche detta "**ARP Table**" degli host.

Possiamo consultare la ARP Table sul nostro host Windows o Linux con il comando *arp*:

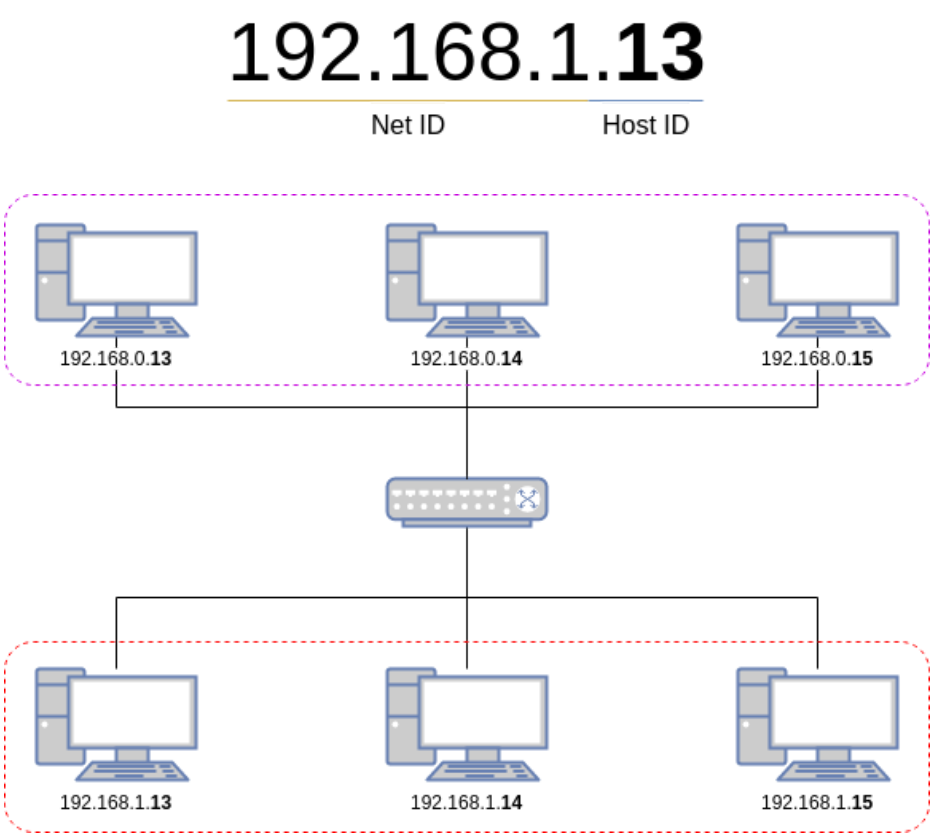
```
C:\Users\Administrator>arp -a

Interface: 192.168.0.72 --- 0x3
  Internet Address      Physical Address      Type
  192.168.0.1           e4-1f-13-c1-6a-5b     dynamic
  192.168.0.5           00-21-9b-19-f6-30     dynamic
  192.168.0.6           6c-3b-e5-18-46-e5     dynamic
  192.168.0.8           00-21-9b-19-a1-ae     dynamic
```

Come funziona un indirizzo IP:
Net ID e Host ID

L'indirizzo IP contiene due informazioni:

- il nome della **rete** (Net ID)
- il nome del **singolo host** (Host ID):



In questa immagine sono presenti **due reti**: la rete **192.168.0**.0 e la rete **192.168.1**.0

Tutti i computer di ciascuna di queste due reti possono comunicare tra loro, ma nessun computer della rete **192.168.0**.0 può comunicare con alcun computer della rete **192.168.1**.0. (Vedremo in seguito i come e i perché)

Classi di Indirizzi IP

Possiamo **arbitrariamente decidere come ripartire NetID e HostID**!

Ad esempio, possiamo avere indirizzi in cui:

- 24 bit indicano il nome della rete, i restanti 8 l'host
- 16 bit per la rete, 16 per l'host
- 8 bit per la rete, 24 per l'host

Fissiamo per un momento l'indirizzo e spostiamo la netmask per capire come cambia:

Classe C — 8 8 8 — 192.168.1.**13**/24

Classe B — 8 8 — 192.168.**1.13**/16

Classe A — 8 — 192.**168.1.13**/8

Gli indirizzi di **classe A** hanno **netmask 8**, quelli di **classe B** hanno **16** e quelli di **classe C 24**.

⚠️ La tabella seguente riassume il **range di indirizzi riservato ad ogni classe** ⚠️

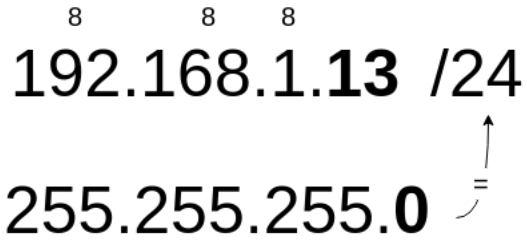
Classe	**Netmask** (CIDR)	Indirizzo iniziale	Indirizzo finale
A (riservato IANA)	8	0.0.0.0	0.255.255.255
A	**8**	1.0.0.0	126.255.255.255
A (loopback)	8	127.0.0.0	127.255.255.255
B	**16**	128.0.0.0	191.255.255.255
C	**24**	192.0.0.0	223.255.255.255
D	-	224.0.0.0	239.255.255.255
E	-	240.0.0.0	255.255.255.255

Questo vi aiuterà a determinare immediatamente la classe di appartenenza di ciascun indirizzo IP.
ES: l'indirizzo **88.50.95.140** è di classe A perché ricade nel range 1.0.0.0 … 126.255.255.255.

NOTA: Le classi di indirizzi IP sono una formalità usata per dividere lo spazio di indirizzamento IPv4 introdotta nel 1981 e usata fino all'introduzione di CIDR nel 1993.

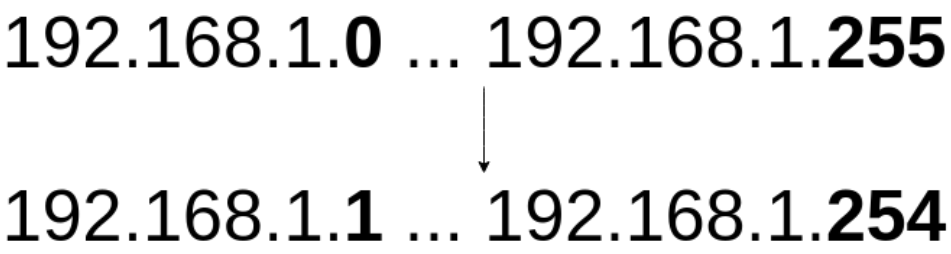
Notazione esplicita

la maschera di bit può essere rappresentata esplicitamente come quartetto di numeri rappresentabili con 8 bit (ovvero da 0 a 255) nella maniera seguente:



Esempio sulle subnet

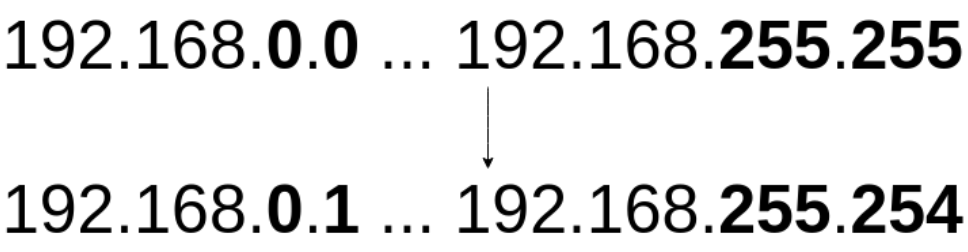
La seguente è una classica rete di classe C (prefisso di rete a 24 bit):
⇒ possiamo avere fino a 256 indirizzi, da 0 a 255:



⇒ Il primo e l'ultimo (**0** e **255**) sono riservati e non possono essere assegnati a nessun host:
- ⇒ **0** indica la rete senza riferirsi a nessun host
- ⇒ **255** è l'indirizzo di broadcast

⇒ In questa rete potremo avere **massimo di 254 host** (256-2).

Per contenere più di 254 host in una unica rete, possiamo usare la netmask 16:



⇒ Il primo e l'ultimo indirizzo (**0.0** e **255.255**) sono speciali e non possono essere usati
⇒ gli indirizzi IP assegnabili vanno da **0.1** a **255.254**

Assegnamento degli IP

L'indirizzo IP può essere assegnato:

- Dinamicamente, da un server DHCP sulla stessa rete
- Staticamente, tramite file di configurazione sull'host

Indirizzi speciali

Alcuni indirizzi sono "speciali" nel senso che non si riferiscono ad un host sulla rete ma hanno una funzione diversa:
ES:

127.0.0.1	→ "questo host" (localhost)
0.0.0.0	→ indirizzo non valido: "tutti gli IP di questo host" (ambito srv)
192.168.1.255	→ Indirizzo di broadcast della rete 192.168.1.0
255.255.255.255	→ Indirizzo di broadcast della rete in cui siamo

Altre classi di indirizzi

Classe D:	da 224.0.0.0 a 239.255.255.255	(indirizzi riservati per multicast)
Classe E	da 240.0.0.0 a 255.255.255.254	(indirizzi riservati per esperimenti futuri)

Indirizzi classless e CIDR

La ripartizione in classi è molto rigida perché si passa da reti con 250 host (Classe C) a reti con 65534 host (Classe B) a reti con milioni di host (classe A).

⇒ Possiamo definire reti con maggiore granularità, spezzando ulteriormente la *subnet mask*!

8 8 8
192.168.1.**13** /24

8 8 7
192.168.1.**13** /23

Specificando una netmask **/23** stiamo togliendo un bit al prefisso di rete, e lasciando un bit in più agli host, che ora sono 2^9 - 2 = 510

Ora gli indirizzi per gli host vanno da 192.168.0.1 fino a 192.168.1.254
Questa pratica è detta ***supernetting***

Subnetting e Supernetting

supernetting*:* Aumentare le dimensioni di una rete riducendo la subnet mask
subnetting: Spezzare una rete in tante piccole sottoreti aumentando la subnet mask

La notazione che abbiamo usato è la **notazione CIDR** (Classless Inter-Domain Routing).

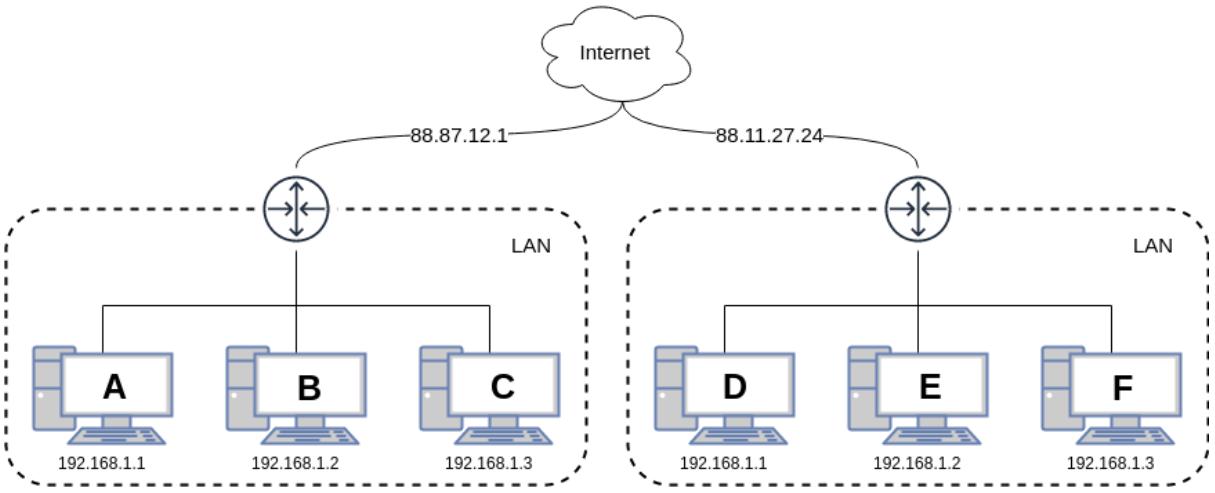
Indirizzi non routable e reti semi-private

Dato il numero sempre crescente di dispositivi connessi alla rete, IANA ha definito degli **spazi di indirizzamento *privati***, ovvero dei "range" di indirizzi **ad uso locale**.

Questi sono anche detti **indirizzi *non routable*** perché vengono scartati automaticamente da tutti i router su Internet (AS e ISP).

Classe A:	[10.0.0.0 - 10.255.255.255]	(10.0.0.0**/8**)	- 1 rete
Classe B:	[172.16.0.0 - 172.31.255.255]	(172.16.0.0**/12**)	- 16 reti
Classe C:	[192.168.0.0 - 192.168.255.255]	(192.168.0.0**/16)**	- 256 reti

Ogni casa / impresa / ufficio … può usare questi stessi indirizzi localmente, e **uscire su internet con un unico indirizzo IP**: quello del proprio **modem router**:



Questo sistema:

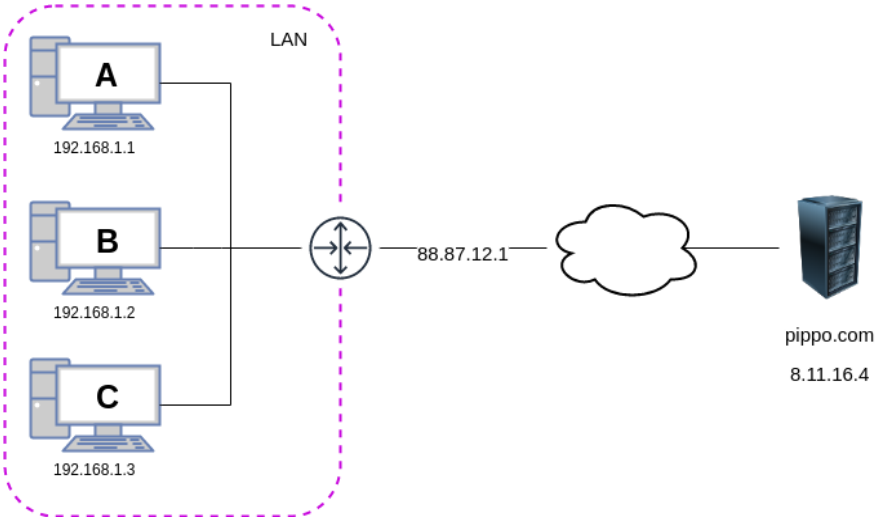
- Riduce l'uso degli indirizzi IP pubblici
- Non espone direttamente gli host su Internet (**vantaggio per la sicurezza!**)

ES: L'host A (B, C, …) non sarà raggiungibile dalla rete esterna!

⇒ Questo tipo di rete si dice "**semi-privata**".

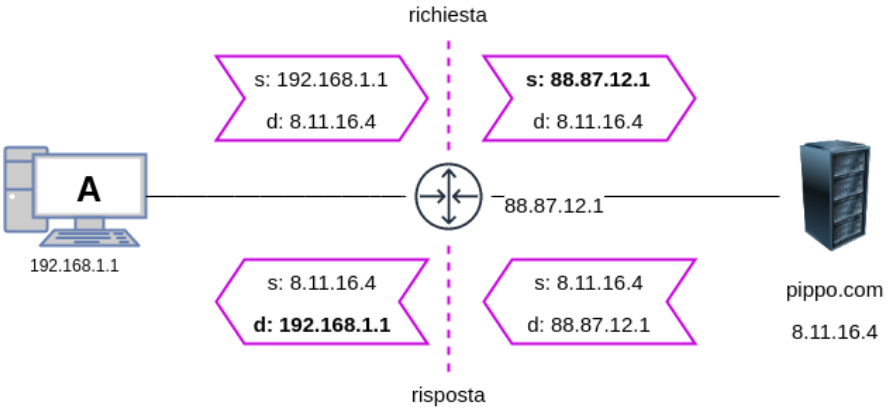
Ma in un certo senso, A deve essere raggiungibile, altrimenti come navighiamo?

NATTING



ES: Dal computer A voglio visitare il sito pippo.com

1. A manda al mio router un *datagram IP* con l'indirizzo di destinazione di pippo.com
2. il mio router, inoltrando il datagram verso la rete esterna, **lo modifica sostituendo l'indirizzo IP del mittente** (locale) **con il proprio** (pubblico).

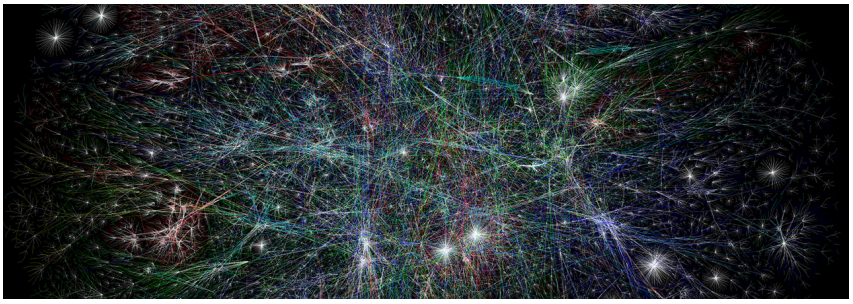


- pippo.com invierà la risposta all'indirizzo IP pubblico del (mio) router.
  (stando al datagram IP, è da quell'indirizzo che è pervenuta la richiesta).
- Il mio router si vede arrivare un datagram **destinato al lui**!
- Il mio router ricorda che ad originare la richiesta era stato A, e **modifica il datagram sostituendo l'IP del destinatario** con quello di A, e inoltra il datagram ad A.

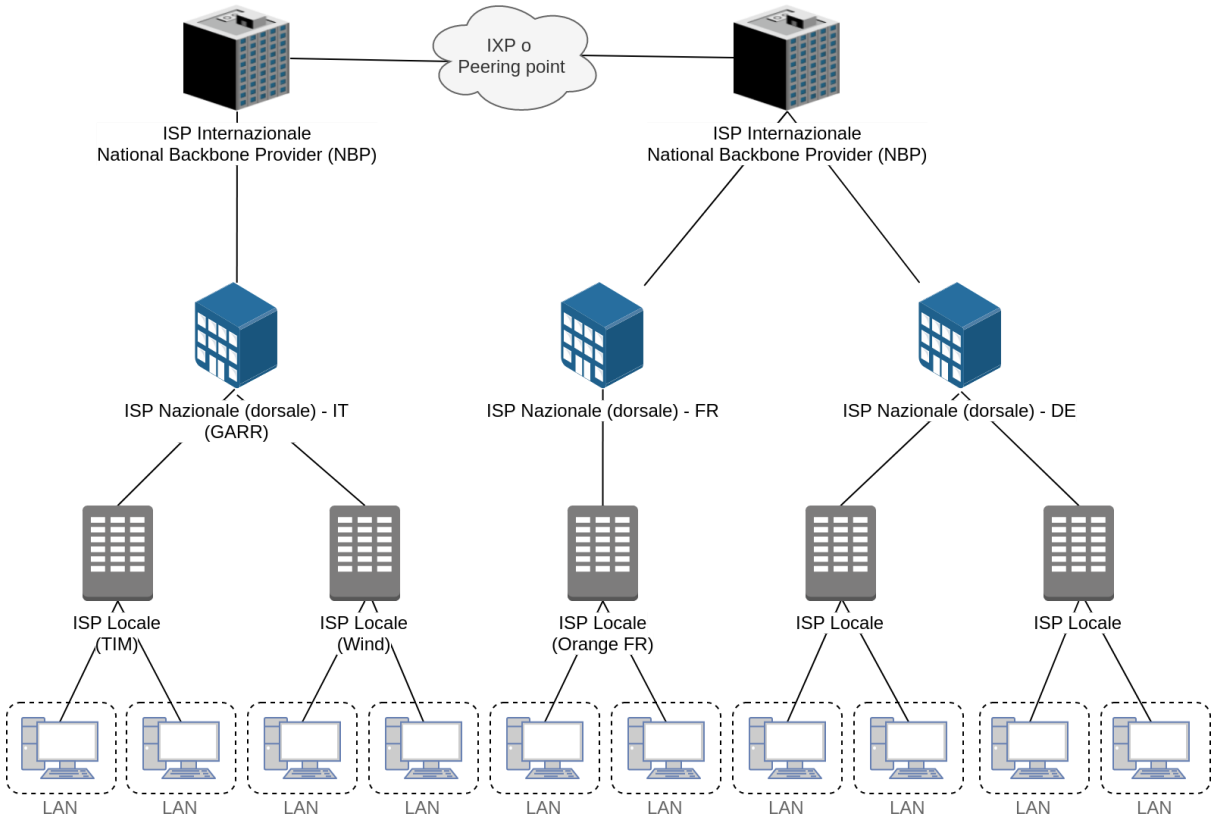
Quanto è appena successo si chiama **NAT** (Network Address Translation) ovvero **il mio router ha tradotto l'IP di A** in un IP pubblico (routable) per circolare su internet, e ha poi fatto il processo inverso per il messaggio di risposta.

Questa pratica è detta ***source natting***. Questo è come navigate in Internet da casa vostra!

Cos’è Internet?



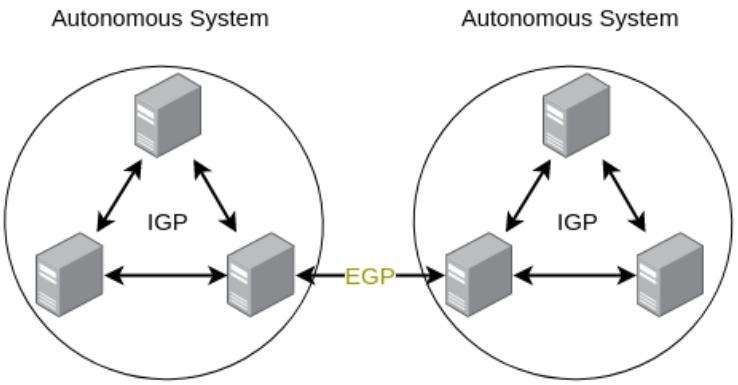
Un enorme agglomerato di reti.



Backbone: enormi reti che coprono **distanze intercontinentali** per collegare stati e continenti.

Organizzativamente, Internet è un agglomerato di oltre 50’000 **Autonomous Systems**, dai più “piccoli” su scala nazionale, ai più grandi su scala intercontinentale.

Cosa sono gli Autonomous System?

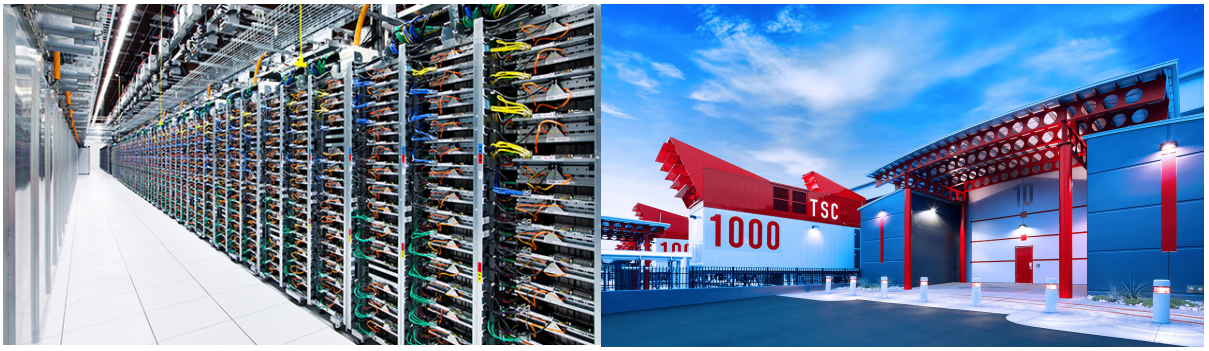


Sono enti o consorzi teoricamente indipendenti che:

- Gestiscono “regioni” di indirizzi e insiemi di reti
- internamente utilizzano lo stesso protocollo di routing
- Dall’esterno vengono visti come un’unica entità.

Gli AS si collegano tra loro tramite:

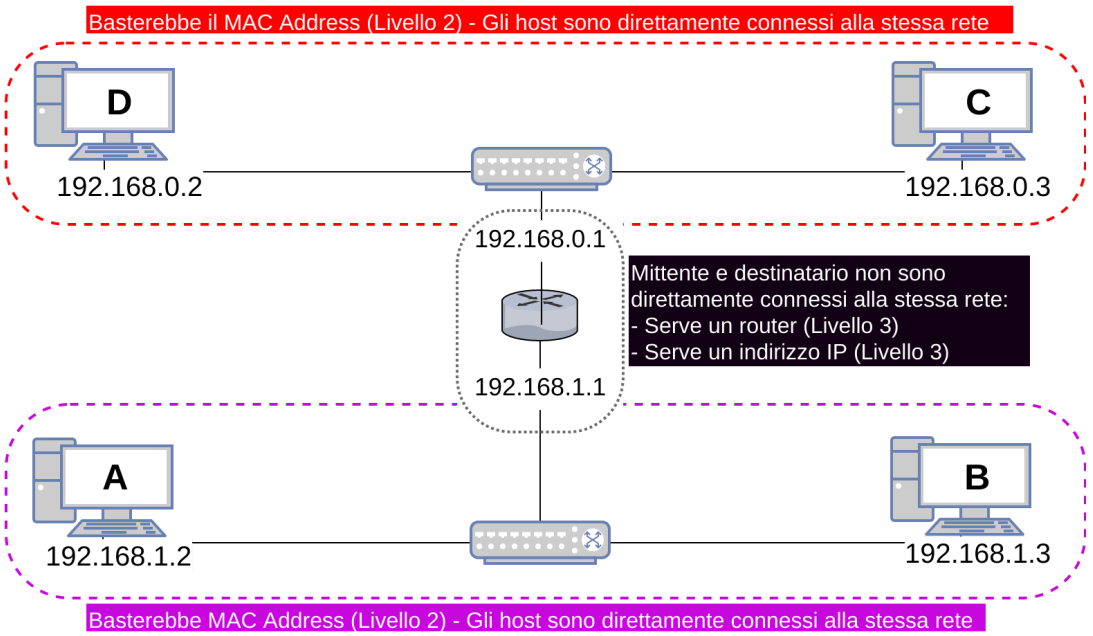
- Peering Point (**PP**)
    - Le spese possono essere divise a vantaggio di entrambi
    - Oppure un AS paga un altro AS per far transitare il traffico
- Internet Exchange Point (**IXP**)
    - Solitamente consorzi indipendenti senza scopo di lucro
    - A volte supportati da finanziamenti pubblici



AMS-IX (Amsterdam) e SuperNAP (Las Vegas)

Router

Serve a interconnettere due (o più) reti separate. Ha almeno due interfacce di rete: una rivolta verso verso la prima rete e una rivolta verso una seconda rete.



Problema del Routing

Scegliere il percorso nella rete attraverso il quale consegnare i pacchetti.

Ogni router si comporta così:

- Se sa dove si trova l'indirizzo di destinazione, inoltra il pacchetto in quella direzione
- Altrimenti inoltra il pacchetto al proprio default gateway

Questo procedimento si ripete per ciascun router fino a raggiungere l'host di destinazione.

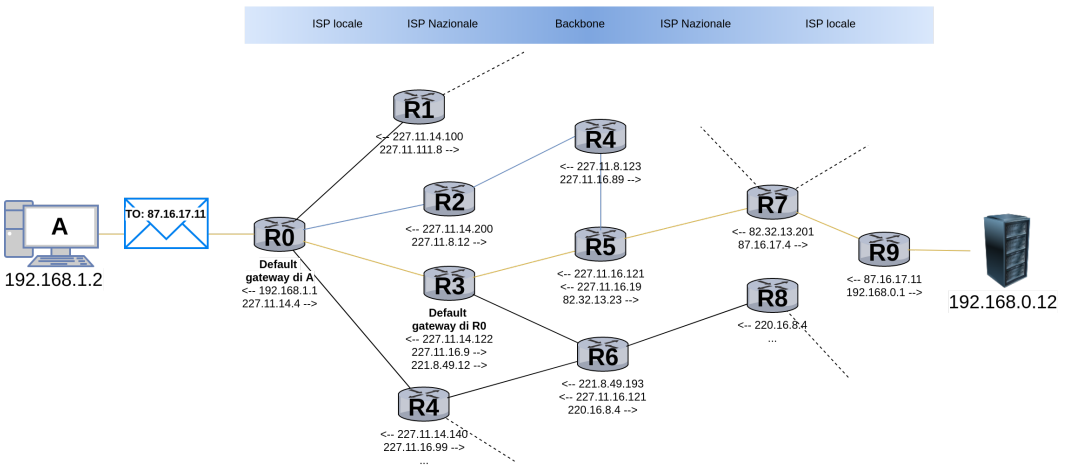
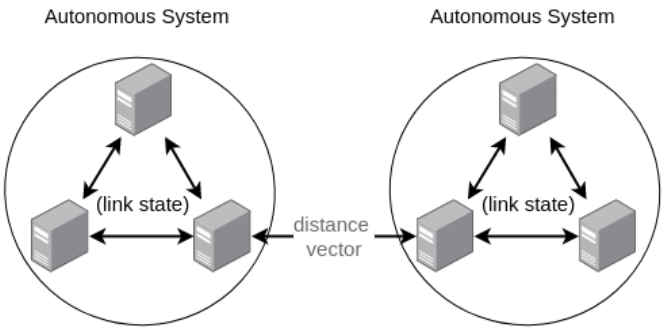


Tabella di routing: memorizza quali nodi portano in quale segmento di rete.

Routing Globale e Locale

Ci sono due classi di algoritmi di routing:

- Algoritmi di routing **globale**
    - Tutti i nodi conoscono lo stato dell'intera rete
    - ES: Link state protocol
- Algoritmi di routing **locale**
    - Ogni nodo comunica il suo stato ai vicini
    - ES: Distance vector protocol



Entrambe le tipologie possono essere usate sia per il routing interno che esterno agli AS.

- Ad uso interno sono spesso preferiti gli algoritmi di tipo *link state*
- Ad uso intra-AS sono preferiti gli algoritmi di tipo *distance vector*

ICMP

Internet **C**ontrol **M**essage **P**rotocol

Protocollo per la diagnostica di base delle reti come il controllo sulla raggiungibilità di un host per il riscontro di malfunzionamenti.

Prevede una serie di codici di controllo come:

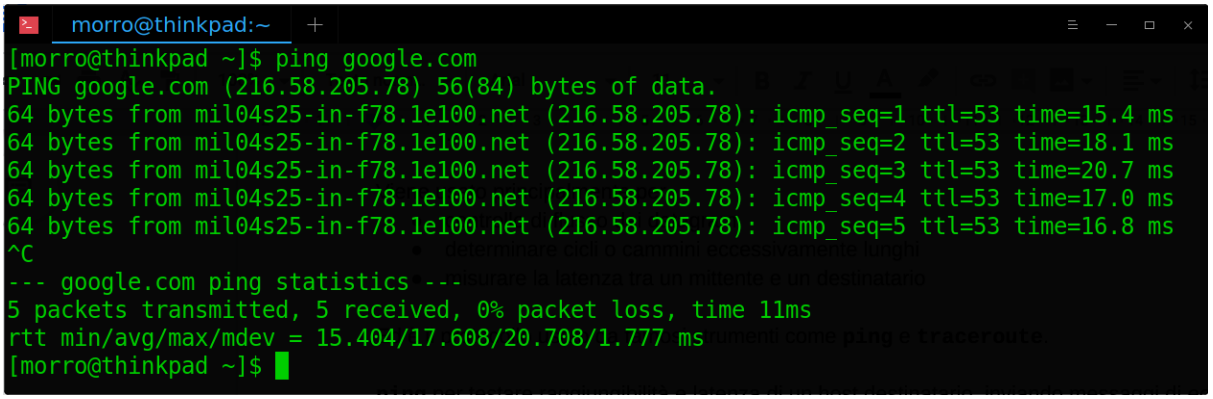
- 0 Destination network unreachable
- 1 Destination host unreachable
- 2 Destination protocol unreachable
- 3 Destination port unreachable
- …

Viene usato principalmente per

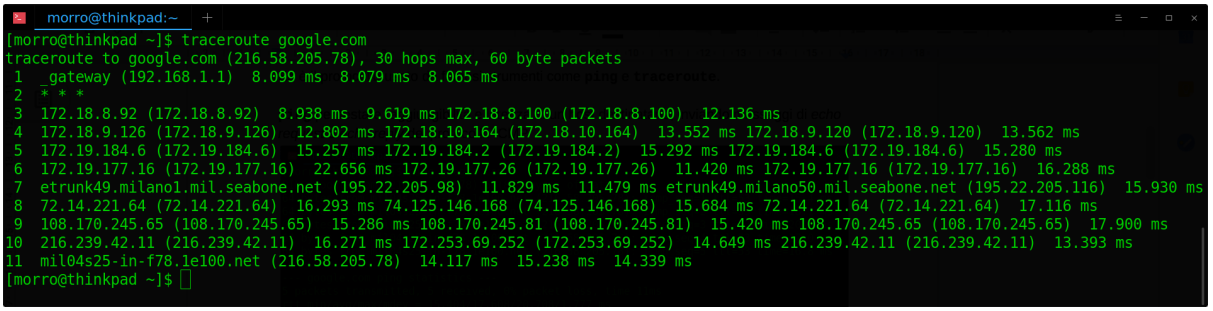
- controllo di flusso dei datagram
- determinare cicli o cammini eccessivamente lunghi
- misurare la latenza tra un mittente e un destinatario

Ed è il protocollo usato da famosi strumenti come **`ping`** e **`traceroute`**.

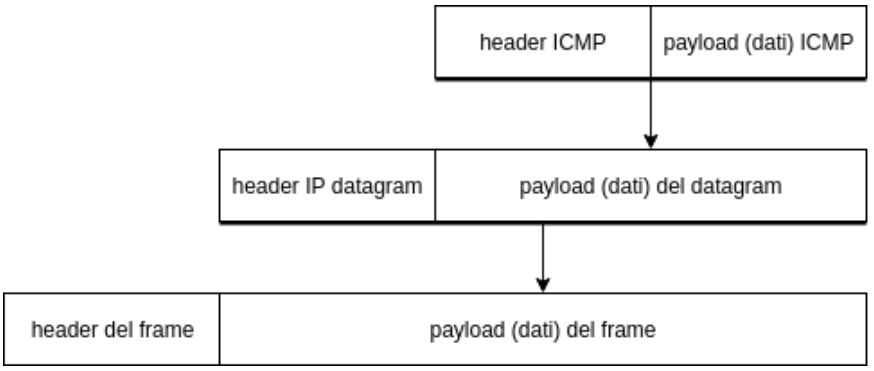
`ping` per testare raggiungibilità e latenza di un host destinatario, inviando messaggi di *echo request* e *echo reply* del protocollo ICMP



`traceroute` per tracciare il cammino da un host A ad un host B. Usa il campo TTL del datagramma IP, quindi se un percorso è eccessivamente lungo e TTL raggiunge lo 0, A riceve un errore ICMP adeguato



Come al solito c'è l'incapsulamento. Un messaggio ICMP, come qualsiasi altro dato trasportato a livello 3, viene incapsulato in un datagramma IP, che a sua volta è incapsulato in un frame ethernet per il trasporto:



Gestione degli indirizzi

1986: il governo USA creava la Internet Assigned Numbers Authority (IANA)

⇒ IANA aveva la giurisdizione sugli indirizzi IP
⇒ INTERNIC (Internet Network Information Center) li distribuiva.

A livello “locale” gli indirizzi si ottenevano da un provider che aveva a disposizione dei range di indirizzi su delega di INTERNIC

1998: il governo americano riconosce l’autorità della Internet Corporation for Assigned Names and Numbers (ICANN)

IANA è ora controllata da ICANN, che ne incorpora tutte le responsabilità ma delega a IANA alcune funzioni di gestione, come la l’allocazione dello spazio degli indirizzi IP in collaborazione con i 5 Regional Internet Registry (RIR):

- AfrNIC (Africa)
- APNIC (Asia/pacifico)
- ARIN (Nord america)
- LACNIC (America latina)
- RIPE NCC (Europa, medio oriente e asia centrale)

IANA gestisce anche il Servizio di registrazione per gli identificativi dei numeri di porta dei protocolli ed è responsabile della gestione della DNS root zone.

Ricapitolando:

- Un range di indirizzi IP è assegnato agli ISP da IANA/ICANN
- Una organizzazione richiede un indirizzo IP a un ISP
- Internamente all'organizzazione, gli IP locali degli host sono assegnati in maniera indipendente dall'amministratore di rete dell'organizzazione stessa