

Laboratorio di Reti e Sistemi Distribuiti

7: Spazio degli indirizzi IPv4

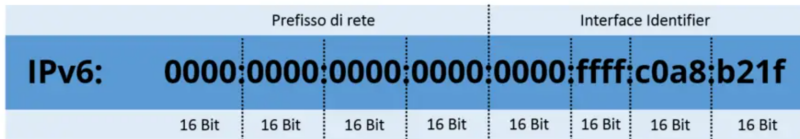
Roberto Marino, PhD¹
`roberto.marino@unime.it`

¹Dipartimento di Matematica, Informatica, Fisica e Scienze della Terra
Future Computing Research Laboratory
Università di Messina

Last Update: 12th March 2025

Spazi degli indirizzi IP

Lo spazio degli indirizzi IP (IP address space) si riferisce **all'insieme di tutti gli indirizzi IP disponibili per un determinato protocollo**, come IPv4 o IPv6. Al momento non ci occuperemo di IPV6.



La **maschera di rete** (o **subnet mask**) è un valore numerico che definisce quali parti di un indirizzo IP identificano la **rete** e quali identificano l'**host**. Separando l'indirizzo IP in:

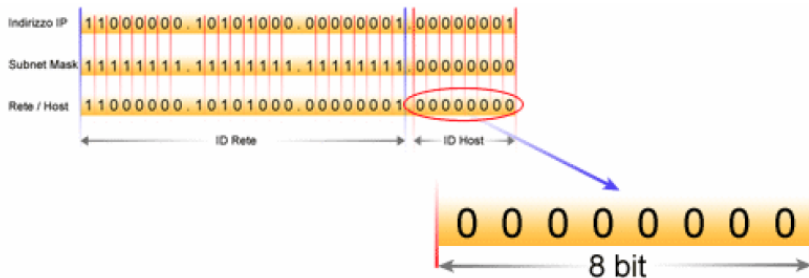
- **Network ID**: Identifica la rete.
- **Host ID**: Identifica il dispositivo specifico.

Esempio di utilizzo

I bit a 1 identificano la rete, i bit a 0 l'host. Esempio:

- **IP:** 192.168.1.10
- **Maschera:** 255.255.255.0 (/24)

Si realizza un AND bit a bit tra maschera che permette di separare Network ID da Host ID.



Le maschere di rete permettono di partizionare lo spazio di indirizzi IP in **sottospazi**
In linea di massima a noi interessano tre sottospazi:

- ① Spazio degli indirizzi **IP Pubblici** (Classfull vs Classless/CIDR)
- ② Spazio degli indirizzi **IP Privati**
- ③ Spazio degli indirizzi **IP Riservati**

Classfull addressing

Introdotta dall'RFC 791 (IP) nel 1981 è ormai obsoleta, definisce gli **indirizzi ip pubblici, o routabili o instradabili**.



Indirizzi IP classe A



Indirizzi IP classe B



Indirizzi IP classe C

Nota bene

Gli indirizzi IP pubblici, a prescindere dal partizionamento classfull o classless sono **UNIVOCI** (possono essere affidati ad una sola interfaccia di rete pubblica).

IP pubblici di classe A (Classfull)

- **Range:** 1.0.0.0 — 126.255.255.255
- **Maschera:** /8 (255.0.0.0)
- **Struttura binaria:** Il primo bit è 0 (es. 0xxxxxxx.xxxxxxxx.xxxxxxxx.xxxxxxxx)
- **Reti disponibili:** 126
- **Host per rete:** $2^{24} - 2 = 16.777.214$
- **Nota bene:** 127.0.0.0/8 è riservato per il loopback (es. 127.0.0.1)

Sottraggo due host per escludere indirizzo di rete ed indirizzo di broadcast

IP pubblici di classe B (Classfull)

- **Range:** 128.0.0.0 — 191.255.255.255
- **Maschera:** /16 (255.255.0.0)
- **Struttura binaria:** I primi due bit sono 10 (es. 10xxxxxx.xxxxxxxx.xxxxxxxx.xxxxxxxx)
- **Reti disponibili:** $2^{14} = 16.384$
- **Host per rete:** $2^{16} - 2 = 65.534$

Sottraggo due host per escludere indirizzo di rete ed indirizzo di broadcast

IP pubblici di classe C (Classfull)

- **Range:** 192.0.0.0 – 223.255.255.255
- **Maschera:** /24 (255.255.255.0)
- **Struttura binaria:** I primi tre bit sono 110 (es. 110xxxxx.xxxxxxxx.xxxxxxxx.xxxxxxxx)
- **Reti disponibili:** $2^{21} = 2.097.152$
- **Host per rete:** $2^8 - 2 = 254$

Sottraggo due host per escludere indirizzo di rete ed indirizzo di broadcast

Gli indirizzi IP privati (RFC 1918), **noti anche come indirizzi IP non instradabili**, sono un insieme di intervalli di indirizzi IP riservati per l'utilizzo della rete privata. **Questi indirizzi non possono essere utilizzati su Internet pubblico (per questo motivo sono esclusi dallo spazio di indirizzamento pubblico).** Il motivo di questa restrizione è prevenire conflitti e problemi di routing che potrebbero verificarsi se questi indirizzi privati dovessero essere utilizzati pubblicamente.

Gli intervalli di indirizzi IP privati definiti nella RFC 1918 sono i seguenti:

- ❶ da 10.0.0.0 a 10.255.255.255 (10.0.0.0/8)
- ❷ da 172.16.0.0 a 172.31.255.255 (172.16.0.0/12)
- ❸ da 192.168.0.0 a 192.168.255.255 (192.168.0.0/16)

Classe D ed E (Multicast e Riservati)

Classe D: Range 224.0.0.0 — 239.255.255.255 (multicast)

Classe E: Range 240.0.0.0 — 255.255.255.255 (sperimentale)

Pubblici o privati?

Gli indirizzi multicast (vs unicast) non sono né "pubblici" né "privati" nel senso tradizionale degli indirizzi unicast (come gli IPv4 privati 10.0.0.0/8 o gli IPv4 pubblici). Hanno una natura speciale, legata al loro scopo di comunicazione uno-a-molti. Vengono spesso definiti come **indirizzi di gruppo**.

Experimental addressing

La Classe E è una categoria di indirizzi IPv4 riservata, definita nel vecchio sistema classful addressing. A differenza delle classi A, B e C (utilizzate per la comunicazione unicast) e della Classe D (multicast), la Classe E non è mai stata assegnata per uso generale. Il suo scopo originale era sperimentale o futuro, ma è rimasta sostanzialmente inutilizzata.

Il **CIDR (Classless Inter-Domain Routing)** è un metodo introdotto nel 1993 per sostituire il vecchio sistema classful addressing (classi A, B, C). Permette di suddividere lo spazio degli indirizzi IP in blocchi di dimensioni variabili (subnet), superando le limitazioni delle classi predefinite.

Perché è stato introdotto?

Esaurimento IPv4: Le classi fisse (es. Classe B con 65k host) portavano a sprechi di indirizzi.

Flessibilità: Creare sottoreti di qualsiasi dimensione (es. una rete da 512 host con /23).

Indirizzamento

L'indirizzamento nelle reti di calcolatori si riferisce ai metodi utilizzati per identificare e raggiungere dispositivi o servizi. Esistono due approcci principali:

- 1 **indirizzamento diretto**
- 2 **indirizzamento indiretto**

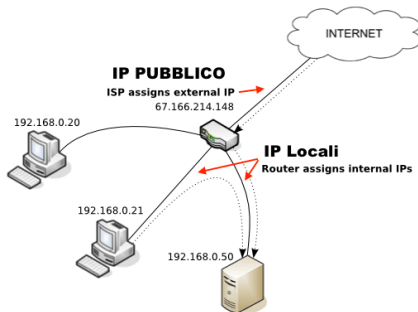


Figure: Rete interna vs Rete Esterna

Avviene quando il computer di destinazione di un pacchetto IP si trova sulla stessa rete locale del mittente. Il software di rete IP posto sul computer mittente non deve eseguire alcun instradamento, ma ottenere direttamente l'indirizzo hardware a 48 bit del destinatario usando il protocollo ARP (Address Resolution Protocol, Protocollo di Risoluzione degli Indirizzi). Dopo aver eseguito questo protocollo, i computer mittente e destinatario dispongono dei rispettivi indirizzi a 48 bit e possono comunicare tra loro inviando i pacchetti IP all'interno di frame Ethernet sulla rete locale.

Quando il computer A spedisce un pacchetto IP a B, il pacchetto IP viaggia **all'interno di un frame Ethernet (incapsulamento)**; l'intestazione del pacchetto IP contiene l'indirizzo IP di A come indirizzo IP sorgente, e l'intestazione del frame Ethernet contiene l'indirizzo Ethernet a 48 bit di A come indirizzo Ethernet sorgente. Analogamente, l'intestazione IP contiene l'indirizzo IP di B come indirizzo IP di destinazione e l'intestazione del frame Ethernet contiene l'indirizzo Ethernet di B come indirizzo Ethernet di destinazione.

Quando il modulo IP di B riceve il pacchetto IP da A, **confronta l'indirizzo IP di destinazione con il suo**, quindi passa il datagramma al protocollo di livello superiore.

Address Resolution Protocol

In realtà gli host di una rete non conoscono **a-priori** gli indirizzi MAC di tutte le destinazioni ma costruiscono una tabella nel tempo (caching) grazie al protocollo ARP (Address Resolution Protocol)

ARP Request

Chi ha l'IP 192.168.1.20? Rispondi con il tuo MAC address!

Arp Reply

Sono io!! Questo è il mio MAC address!!

Address Resolution Protocol

Siano Host A (IP: 192.168.1.10) e Host B (IP: 192.168.1.20), sulla stessa rete LAN. Se Host A vuole inviare un pacchetto direttamente a Host B:

- 1 **Host A** conosce l'IP di destinazione (192.168.1.20), ma non il MAC address corrispondente.
- 2 **Host A** invia un ARP Request in broadcast alla rete, chiedendo: "Chi ha l'IP 192.168.1.20? Rispondi con il tuo MAC address!".
- 3 **Host B**, riconoscendo il proprio IP nella richiesta, risponde con un ARP Reply contenente il suo MAC address.
- 4 **Host A** memorizza l'associazione IP \rightarrow MAC in una tabella ARP cache per comunicazioni future.

Ora, Host A può inviare frame Ethernet direttamente a Host B usando il suo MAC address.

Ruolo di ARP nell'indirizzamento diretto

- **Abilita la comunicazione diretta a Layer 2:** Senza ARP, anche conoscendo l'IP di un dispositivo, non sarebbe possibile inviargli dati a livello fisico (Ethernet).
- **Mantiene l'efficienza:** Le tabelle ARP cache riducono il traffico broadcast, memorizzando le associazioni IP-MAC

Comando ARP (visualizzare, inserire, cancellare entry arp)

arp -a (visualizza la tabella cache)

arp -help

Indirizzamento indiretto

Nell'indirizzamento indiretto, un dispositivo (es: un PC) non comunica direttamente con il destinatario finale, **ma utilizza un router o gateway come intermediario per raggiungere reti esterne (es: Internet)**. In questo contesto, ARP non risolve l'indirizzo MAC del destinatario finale, ma quello del gateway, permettendo al pacchetto di essere instradato verso la rete esterna.

Livello 3

Host A (IP: 192.168.1.10, rete locale) vuole inviare un pacchetto a **Host B (IP: 8.8.8.8, rete esterna)**.

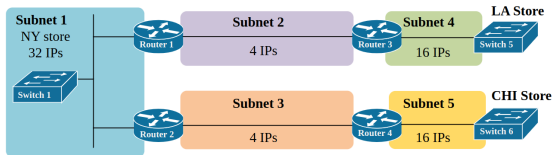
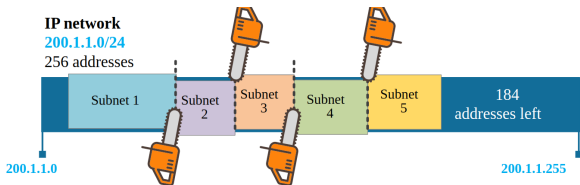
Host A sa che 8.8.8.8 non è nella sua rete locale (grazie alla subnet mask), quindi usa il **gateway predefinito** (es: router con IP 192.168.1.1).

Risoluzione ARP (Bridge tra livello 3 e livello 2)

- 1 Host A verifica se conosce il MAC address del gateway (192.168.1.1) nella sua tabella ARP.
- 2 Se non lo trova, invia una ARP Request in broadcast: "Chi ha l'IP 192.168.1.1? Rispondi con il tuo MAC!".
- 3 Il router risponde con il suo MAC address (es: AA:BB:CC:DD:EE:FF).
- 4 Host A invia il pacchetto al router, usando il MAC destinazione: AA:BB:CC:DD:EE:FF (MAC del gateway) e l' IP destinazione: 8.8.8.8 (indirizzo finale).
- 5 Il router si occupa di inoltrare il pacchetto verso l'esterno (usando la sua routing table e altri protocolli).

Subnetting

Il **subnetting** è la pratica di **suddividere una rete IP in sottoreti (subnet) più piccole**, ottimizzando l'uso degli indirizzi, migliorando la sicurezza e riducendo il traffico broadcast. Si basa sulla modifica della subnet mask per **"rubare"** bit alla parte host dell'indirizzo IP e usarli per creare reti logiche separate.



Subnetting: Esempio

- 1 Determinare il numero di sottoreti necessarie (es: 4 subnet).
- 2 Calcolare i bit necessari per le subnet: Ad esempio con 4 subnet servono $\log_2(4) = 2$
- 3 Modificare la subnet mask: Esempio: Da /24 (255.255.255.0) a /26 (255.255.255.192).
- 4 Calcolare gli intervalli di host validi per ogni subnet.

Comandi utili

```
ipcalc
```

```
ip route add default via 192.168.1.1 dev eth0
```

Rete originale: 192.168.1.0/24 (254 host possibili)

Obiettivo: Creare 4 subnet con almeno 50 host ciascuna

Bit necessari per le subnet: 2, tramite logaritmo

Maschera Originale: 24 bit \rightarrow Nuova Maschera: $24 + 2 = 26$ bit
(255.255.255.192)

Nuove sottoreti

- Subnet 1: 192.168.1.0/26 \rightarrow Host: 192.168.1.1 - 192.168.1.62
- Subnet 2: 192.168.1.64/26 \rightarrow Host: 192.168.1.65 - 192.168.1.126
- Subnet 3: 192.168.1.128/26 \rightarrow Host: 192.168.1.129 - 192.168.1.190
- Subnet 4: 192.168.1.192/26 \rightarrow Host: 192.168.1.193 - 192.168.1.254