

# Introduzione al TCP/IP

Il nome TCP/IP rappresenta un sistema di protocolli di comunicazione basati su IP e si tratta di quanto utilizzato normalmente negli ambienti Unix.

## 246.1 TCP/IP e il modello ISO-OSI

Il protocollo IP si colloca al terzo livello ISO-OSI, mentre TCP si colloca al di sopra di questo e utilizza IP al livello inferiore. In realtà, il TCP/IP annovera anche altri protocolli importanti, che comunque sono impliciti nella denominazione TCP/IP.

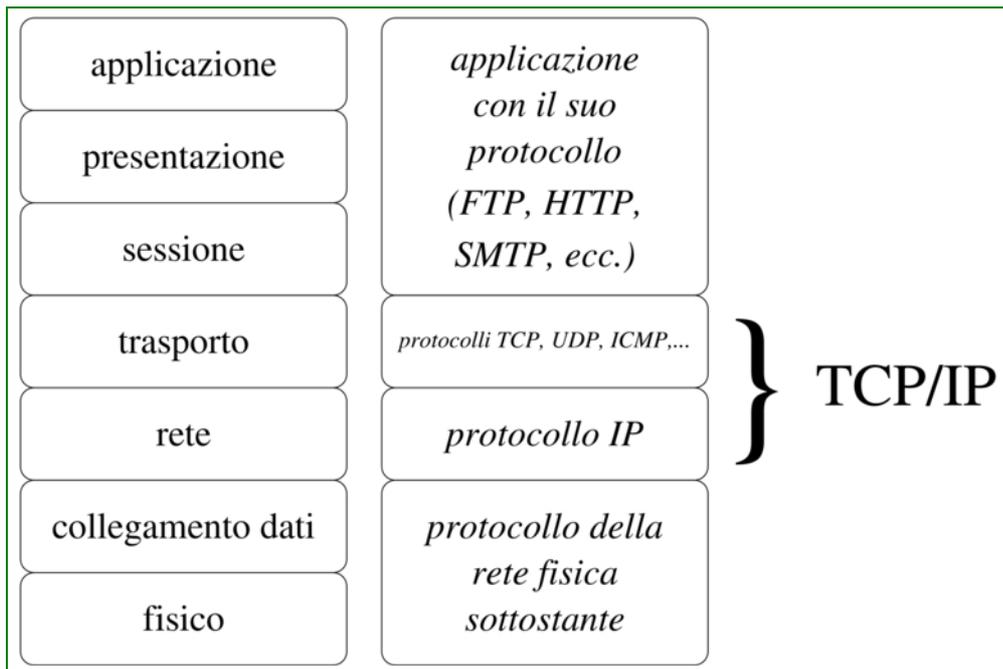
I vari aspetti del sistema di protocolli TCP/IP si possono apprendere mano a mano che si studiano gli indirizzamenti e i servizi di rete che vengono resi disponibili. In questa fase conviene rivedere il modello ISO-OSI in abbinamento al TCP/IP.

Tabella [246.1](#). Modello ISO-OSI di suddivisione delle competenze di un sistema TCP/IP.

Livello	Definizione	Descrizione
7	Applicazione	Applicazioni.
6	Presentazione	Definizione standard del formato dei dati utilizzati.
5	Sessione	Protocolli dei servizi (FTP, HTTP, SMTP, RPC, ecc.).
4	Trasporto	Protocolli TCP, UDP e ICMP.
3	Rete	Protocollo IP.
2	Collegamento dati	Trasmissione e ricezione dati dipendente dal tipo di hardware.
1	Fisico	Hardware.

A parte la descrizione che si fa nel seguito, il TCP/IP vede in pratica solo quattro livelli, che in alcuni casi incorporano più livelli del modello tradizionale. La figura [246.2](#) cerca di semplificare questo abbinamento.

Figura [246.2](#). Abbinamento tra il modello ISO-OSI e la semplicità dei protocolli TCP/IP.



Questo comunque non significa che gli strati del modello tradizionale non esistono. Piuttosto possono essere svolti all'interno di una sola applicazione, oppure sono al di fuori della competenza del protocollo TCP/IP.

1	fisico	Perché si possa avere una connessione con altri nodi, è necessario inizialmente un supporto fisico, composto solitamente da un cavo e da interfacce di comunicazione. La connessione tipica in una rete locale è fatta utilizzando hardware Ethernet. Il cavo o i cavi e le schede Ethernet appartengono a questo primo livello.
2	collegamento dei dati	Il tipo di hardware utilizzato nel primo livello determina il modo in cui avviene effettivamente la comunicazione. Nel caso dell'hardware Ethernet, ogni scheda ha un proprio indirizzo univoco (stabilito dal fabbricante) composto da 48 bit e rappresentato solitamente in forma esadecimale, come nell'esempio seguente:  00:A0:24:77:49:97
3	rete	Per poter avere un tipo di comunicazione indipendente dal supporto fisico utilizzato, è necessaria un'astrazione che riguarda il modo di inviare blocchi di dati, l'indirizzamento di questi e il loro instradamento. Per quanto riguarda il TCP/IP, questo è il livello del protocollo IP, attraverso il quale vengono definiti gli indirizzi e gli instradamenti relativi.  Quando un pacchetto è più grande della dimensione massima trasmissibile in quel tipo di rete fisica utilizzata, è il protocollo IP che si deve prendere cura di scomporlo in segmenti più piccoli e di ricombinarli correttamente alla destinazione.
4	trasporto	A questo livello appartengono i protocolli di comunicazione che si occupano di frammentare e ricomporre i dati, di correggere gli errori e di prevenire intasamenti della rete. I protocolli principali di questo livello sono TCP ( <i>Transmission control protocol</i> ) e UDP ( <i>User datagram protocol</i> ).

	<p>Il protocollo TCP, in qualità di protocollo connesso, oltre alla scomposizione e ricomposizione dei dati, si occupa di verificare e riordinare i dati all'arrivo: i pacchetti persi o errati vengono ritrasmessi e i dati finali vengono ricomposti. Il protocollo UDP, essendo un protocollo non connesso, non esegue alcun controllo.</p> <p>A questo livello si introduce, a fianco dell'indirizzo IP, il numero di porta. Il percorso di un pacchetto ha un'origine, identificata dal numero IP e da una porta, e una destinazione identificata da un altro numero IP e dalla porta relativa. Le porte identificano convenzionalmente dei servizi concessi o richiesti e la gestione di questi riguarda il livello successivo.</p>
5 sessione	<p>Ogni servizio di rete (condivisione del file system, posta elettronica, FTP, ecc.) ha un proprio protocollo, porte di servizio e un meccanismo di trasporto (quelli definiti nel livello inferiore). Ogni sistema può stabilire le proprie regole, anche se in generale è opportuno che i nodi che intendono comunicare utilizzino le stesse porte e gli stessi tipi di trasporto. Questi elementi sono stabiliti dal file <code>/etc/services</code>. Segue una riga di questo file dove si può osservare che il servizio <b>www</b> (HTTP) utilizza la porta 80 per comunicare e il protocollo di trasporto è il TCP:</p> <pre>www      80/tcp</pre> <p>Quando si avvia una comunicazione a questo livello, si parla di sessione. Quindi, si apre o si chiude una sessione.</p>
6 presentazione	<p>I dati che vengono inviati utilizzando le sessioni del livello inferiore devono essere uniformi, indipendentemente dalle caratteristiche fisiche delle macchine che li elaborano. A questo livello si inseriscono normalmente delle librerie in grado di gestire un'eventuale conversione dei dati tra l'applicazione e la sessione di comunicazione.</p>
7 applicazione	<p>L'ultimo livello è quello dell'applicazione che utilizza le risorse di rete. Con la suddivisione delle competenze in così tanti livelli, l'applicazione non ha la necessità di occuparsi della comunicazione; così, in molti casi, anche l'utente può non rendersi conto della sua presenza.</p>

## 246.2 ARP

A livello elementare, la comunicazione attraverso la rete deve avvenire in un modo compatibile con le caratteristiche fisiche di questa. In pratica, le connessioni devono avere una forma di attuazione al secondo livello del modello appena presentato (collegamento dati); i livelli superiori sono solo astrazioni della realtà che c'è effettivamente sotto. Per poter utilizzare un protocollo che si ponga al terzo livello, come nel caso di IP che viene descritto più avanti, occorre un modo per definire un abbinamento tra gli indirizzi di questo protocollo superiore e gli indirizzi fisici delle interfacce utilizzate effettivamente, secondo le specifiche del livello inferiore.

Volendo esprimere la cosa in modo pratico, si può pensare alle interfacce Ethernet, che hanno un sistema di indirizzamento composto da 48 bit. Quando con un protocollo di livello 3 (rete) si vuole contattare un nodo identificato in maniera diversa da quanto previsto al livello 2, se non si conosce l'indirizzo Ethernet, ma ammettendo che tale nodo si trovi nella rete fisica locale, viene inviata una richiesta circolare secondo il protocollo ARP (*Address resolution protocol*).

La richiesta ARP dovrebbe essere ascoltata da tutte le interfacce connesse fisicamente a quella rete fisica e ogni nodo dovrebbe passare tale richiesta al livello 3, in modo da verificare se l'indirizzo richiesto corrisponde al proprio. In questo modo, il nodo che ritiene di essere quello che si sta cercando dovrebbe rispondere, rivelando il proprio indirizzo Ethernet.

Ogni nodo dovrebbe essere in grado di conservare per un certo tempo le corrispondenze tra gli indirizzi di livello 2 con quelli di livello 3, ottenuti durante il funzionamento. Questo viene fatto nella tabella ARP, che comunque va verificata a intervalli regolari.

## 246.3 Indirizzi IPv4

Come descritto nelle sezioni precedenti, al di sopra dei primi due livelli strettamente fisici di comunicazione, si inserisce la rete dal punto di vista di Unix: un insieme di nodi, spesso definiti *host*, identificati da un indirizzo IP. Di questi ne esistono almeno due versioni: IPv4 e IPv6. Il primo è ancora in uso, ma a causa del rapido esaurimento degli indirizzi disponibili nella comunità Internet, è in corso di diffusione l'uso del secondo.

Gli indirizzi IP versione 4, cioè quelli tradizionali, sono composti da una sequenza di 32 bit, suddivisi convenzionalmente in quattro gruppetti di 8 bit, rappresentati in modo decimale separati da un punto. Questo tipo di rappresentazione è definito come: *notazione decimale puntata*. L'esempio seguente corrisponde al codice 1.2.3.4:

```
00000001.00000010.00000011.00000100
```

All'interno di un indirizzo del genere si distinguono due parti: l'indirizzo di rete e l'indirizzo del nodo particolare. Il meccanismo è simile a quello del numero telefonico in cui la prima parte del numero, il prefisso, definisce la zona ovvero il distretto telefonico, mentre il resto identifica l'apparecchio telefonico specifico di quella zona. In pratica, quando viene richiesto un indirizzo IP, si ottiene un indirizzo di rete in funzione della quantità di nodi che si devono connettere. In questo indirizzo una certa quantità di bit nella parte finale sono azzerati: ciò significa che quella parte finale può essere utilizzata per gli indirizzi specifici dei nodi. Per esempio, l'indirizzo di rete potrebbe essere:

```
00000001.00000010.00000011.00000000
```

In tal caso, si potrebbero utilizzare gli ultimi 8 bit per gli indirizzi dei vari nodi.

L'indirizzo di rete, non può identificare un nodo. Quindi, tornando all'esempio, l'indirizzo seguente non può essere usato per identificare anche un nodo:

```
00000001.00000010.00000011.00000000
```

Inoltre, un indirizzo in cui i bit finali lasciati per identificare i nodi siano tutti a uno, identifica un indirizzo *broadcast*, cioè un indirizzo per la trasmissione a tutti i nodi di quella rete:

```
00000001.00000010.00000011.11111111
```

In pratica, rappresenta simultaneamente tutti gli indirizzi che iniziano con 00000001.00000010.00000011. Di conseguenza, un indirizzo broadcast non può essere utilizzato per identificare un nodo.

Naturalmente, i bit che seguono l'indirizzo di rete possono anche essere utilizzati per suddividere la rete in sottoreti. Nel caso di prima, volendo creare due sottoreti utilizzando i primi 2 bit che seguono l'indirizzo di rete originario:

```
xxxxxxxxxxxxxxxxxxxxxxxx.00000000 indirizzo di rete;
xxxxxxxxxxxxxxxxxxxxxxxx.01000000 indirizzo della prima sottorete;
xxxxxxxxxxxxxxxxxxxxxxxx.10000000 indirizzo della seconda sottorete;
xxxxxxxxxxxxxxxxxxxxxxxx.11111111 indirizzo broadcast.
```

In questo esempio, per ogni sottorete, resterebbero 6 bit a disposizione per identificare i nodi: da  $000001_2$  a  $111110_2$ .

Il meccanismo utilizzato per distinguere la parte dell'indirizzo che identifica la rete è quello della **maschera di rete** o *netmask*. La maschera di rete è un indirizzo che viene abbinato all'indirizzo da analizzare con l'operatore booleano AND, per filtrare la parte di bit che interessano. Prima di vedere come funziona il meccanismo, la tabella [246.5](#) può essere utile per ripassare rapidamente le tabelline della verità degli operatori logici principali.

Tabella [246.5](#). Riassunto del funzionamento degli operatori logici principali.

ingresso	ingresso	uscita AND	ingresso	ingresso	uscita OR	ingresso	uscita NOT
0	0	0	0	0	0	0	1
0	1	0	0	1	1	1	0
1	0	0	1	0	1		
1	1	1	1	1	1		

Una maschera di rete che consenta di classificare i primi 24 bit come indirizzo di rete è quella seguente, che coincide con il ben più noto codice 255.255.255.0:

11111111.11111111.11111111.00000000

Utilizzando l'esempio visto in precedenza, abbinando questa maschera di rete si ottiene l'indirizzo di rete:

```
00000001.00000010.00000011.00000100 nodo (1.2.3.4)
11111111.11111111.11111111.00000000 maschera di rete (255.255.255.0)
00000001.00000010.00000011.00000000 indirizzo di rete (1.2.3.0).
```

L'indirizzo che si ottiene abbinando l'indirizzo di un nodo e la sua maschera di rete **invertita** (attraverso l'operatore NOT) con l'operatore AND è l'indirizzo del nodo relativo alla propria rete. Esempio:

```
00000001.00000010.00000011.00000100 nodo (1.2.3.4)
00000000.00000000.00000000.11111111 maschera di rete invertita
(0.0.0.255)
```

00000000.00000000.00000000.00000100 indirizzo relativo (0.0.0.4)

Tabella 246.8. Tabellina di conversione rapida per determinare la parte finale di una maschera di rete secondo la notazione decimale puntata.

Ottetto binario	Ottetto esadecimale	Ottetto decimale
11111111 <sub>2</sub>	FF <sub>16</sub>	255 <sub>10</sub>
11111110 <sub>2</sub>	FE <sub>16</sub>	254 <sub>10</sub>
11111100 <sub>2</sub>	FC <sub>16</sub>	252 <sub>10</sub>
11111000 <sub>2</sub>	F8 <sub>16</sub>	248 <sub>10</sub>
11110000 <sub>2</sub>	F0 <sub>16</sub>	240 <sub>10</sub>
11100000 <sub>2</sub>	E0 <sub>16</sub>	224 <sub>10</sub>
11000000 <sub>2</sub>	C0 <sub>16</sub>	192 <sub>10</sub>
10000000 <sub>2</sub>	80 <sub>16</sub>	128 <sub>10</sub>
00000000 <sub>2</sub>	00 <sub>16</sub>	0 <sub>10</sub>

### 246.3.1 Classi di indirizzi

Gli indirizzi IP versione 4 sono stati classificati in cinque gruppi, a partire dalla lettera «A» fino alla lettera «E».

Tabella 246.9. Classe A. Gli indirizzi di classe A hanno il primo bit a zero, utilizzano i sette bit successivi per identificare l'indirizzo di rete e lasciano i restanti 24 bit per identificare i nodi.

	Binario	Notazione decimale puntata
modello	0rrrrrrr.hhhhhhhh.hhhhhhhh.hhhhhhhh	
da	00000001._____._____._____	1.____.____.____
a	01111111._____._____._____	127.____.____.____

Tabella 246.10. Classe B. Gli indirizzi di classe B hanno il primo bit a uno e il secondo a zero, utilizzano i 14 bit successivi per identificare l'indirizzo di rete e lasciano i restanti 16 bit per identificare i nodi.

	Binario	Notazione decimale puntata
modello	10rrrrrr.rrrrrrrr.hhhhhhhh.hhhhhhhh	
da	10000000.00000001._____._____	128.1.____.____
a	10111111.11111110._____._____	191.254.____.____

Tabella 246.11. Classe C. Gli indirizzi di classe C hanno il primo e il secondo bit a uno e il terzo bit a zero, utilizzano i 21 bit successivi per identificare l'indirizzo di rete e lasciano i restanti 8 bit per identificare i nodi.

	Binario	Notazione decimale puntata
modello	110rrrrr.rrrrrrrr.rrrrrrrr.hhhhhhhh	
da	11000000.00000000.00000001._____	192.0.1.____
a	11011111.11111111.11111110._____	223.255.254.____

Tabella 246.12. Classe D. Gli indirizzi di classe D hanno i primi tre bit a uno e il quarto a zero. Si tratta di una classe destinata a usi speciali.

	Binario	Notazione decimale puntata
modello	1110xxxx.xxxxxxxxxxxxxxxxxx	
da		224.____.____.____
a		239.____.____.____

Tabella 246.13. Classe E. Gli indirizzi di classe E hanno i primi quattro bit a uno e il quinto a zero. Si tratta di una classe destinata a usi speciali.

	Binario	Notazione decimale puntata
modello	11110xxx.xxxxxxxxxxxxxxxxxx	
da		240.____.____.____
a		247.____.____.____

Tabella 246.14. Riepilogo delle classi IPv4.

Prefisso binario	Intervallo di indirizzi in notazione decimale puntata	Impiego
0 <sub>2</sub>	da 1.0.0.0 a 127.255.255.255	Classe A
10 <sub>2</sub>	da 128.0.0.0 a 191.255.255.255	Classe B
110 <sub>2</sub>	da 192.0.0.0 a 223.255.255.255	Classe C
1110 <sub>2</sub>	da 224.0.0.0 a 239.255.255.255	Classe D
11110 <sub>2</sub>	da 240.0.0.0 a 247.255.255.255	Classe E

### 246.3.2 Indirizzi speciali

Alla fine della classe A, gli indirizzi 127.\*.\*.\*, sono riservati per identificare una rete virtuale interna al nodo stesso. All'interno di questa rete si trova un'interfaccia di rete immaginaria connessa su questa stessa rete, corrispondente all'indirizzo 127.0.0.1, mentre gli altri indirizzi di questo gruppo non vengono mai utilizzati.

Per identificare questi indirizzi si parla di *loopback*, anche se questo termine viene usato ancora in altri contesti con significati differenti.

All'interno di ogni nodo, quindi, l'indirizzo 127.0.0.1 corrisponde a se stesso. Serve in particolare per non disturbare la rete quando un programma (che usa la rete) deve fare riferimento a se stesso.

L'indirizzo speciale 0.0.0.0, conosciuto come *default route* è il percorso, o la strada predefinita per l'instradamento dei pacchetti. Si usa spesso la parola chiave **default route** per fare riferimento automaticamente a questo indirizzo particolare.

### 246.3.3 Indirizzi riservati per le reti private

Se non si ha la necessità di rendere accessibili i nodi della propria rete locale alla rete globale Internet, si possono utilizzare alcuni gruppi di indirizzi che sono stati riservati a questo scopo e che non corrispondono a nessun nodo raggiungibile attraverso Internet.

Tabella 246.15. Indirizzi riservati alle reti private.

Classe	Notazione decimale puntata	Binario
A	da 10.0.0.0	00001010.00000000.00000000.00000000
A	a 10.255.255.255	00001010.11111111.11111111.11111111
B	da 172.16.0.0	10101100.00010000.00000000.00000000
B	a 172.31.255.255	10101100.00011111.11111111.11111111
C	da 192.168.0.0	11000000.10101000.00000000.00000000
C	a 192.168.255.255	11000000.10101000.11111111.11111111

### 246.3.4 Sottoreti e instradamento

Quando si scompone la propria rete locale in sottoreti, lo si fa normalmente per raggruppare i nodi in base alle attività che essi condividono. Le sottoreti possono essere immaginate come raggruppamenti di nodi separati che di tanto in tanto hanno la necessità di accedere a nodi situati al di fuori del loro gruppo. Per collegare due sottoreti occorre un nodo con due interfacce di rete, ognuno connesso con una delle due reti, configurato in modo da lasciare passare i pacchetti destinati all'altra rete: questo è un router.

Si osservi che, in questo contesto, il termine *gateway* si usa per indicare il passaggio che devono prendere i pacchetti per raggiungere una certa rete. Pertanto, ciò può rappresentare l'indirizzo, presso la propria rete locale, del router che si occupa di tale instradamento. È però sbagliato confondere il termine *gateway* con router, perché comunque il primo dei due ha un significato generico, non riferito necessariamente al problema dell'instradamento al terzo livello del modello ISO-OSI.

### 246.3.5 Maschere IP e maschere di rete

Il modo normale di rappresentare una maschera degli schemi di indirizzamento di IPv4 è quello della notazione decimale puntata a ottetti, come visto fino a questo punto. Tuttavia, considerato che le maschere servono prevalentemente per definire dei gruppi di indirizzi IP, cioè delle reti (o sottoreti), tali maschere hanno una forma piuttosto semplice: una serie continua di bit a uno e la parte restante di bit a zero. Pertanto, quando si tratta di definire una maschera di rete, potrebbe essere conveniente indicare semplicemente il numero di bit da porre a uno. Per esempio, la classica maschera di rete di classe C, 255.255.255.0, equivale a dire che i primi 24 bit devono essere posti a uno.

La possibilità di rappresentare le maschere di rete in questo modo è apparsa solo in tempi recenti per quanto riguarda IPv4. Quindi, dipende dai programmi di servizio utilizzati effettivamente, il fatto che si possa usare o meno questa forma. In ogni caso, il modo normale di esprimerla è quello di indicare il numero IP seguito da una barra obliqua normale e dal numero di bit a uno della maschera, come per esempio 192.168.1.1/24.

### 246.3.6 Sottoreti particolari in classe C

A causa della penuria di indirizzi IPv4, recentemente si tende a utilizzare la classe C in modo da ottenere il maggior numero di sottoreti possibili. Nella sezione [246.3](#) è stato mostrato un esempio di suddivisione in sottoreti, in cui si utilizzano i primi 2 bit dell'ultimo ottetto per ottenere due reti, che possono raggiungere un massimo di 62 nodi per rete, mentre se si trattasse di una rete unica per tutto l'ottetto finale sarebbe possibile raggiungere 254 nodi.

Se si parte dal presupposto che ogni sottorete abbia il proprio indirizzo broadcast, nel senso che non esiste più un indirizzo broadcast generale, si può fare di meglio, anche se la cosa non è consigliabile in generale.

Maschera di rete a 25 bit, pari a 255.255.255.128, per due sottoreti con 126 nodi ognuna:

```
rrrrrrrr, rrrrrrrr, rrrrrrrr, shhhhhh
```

Rete	IP iniziale	IP finale	Broadcast
x.x.x.0	x.x.x.1	x.x.x.126	x.x.x.127
x.x.x.128	x.x.x.129	x.x.x.254	x.x.x.255

```
rrrrrrrr, rrrrrrrr, rrrrrrrr, sshhhhh
```

Maschera di rete a 26 bit, pari a 255.255.255.192, per quattro sottoreti con 62 nodi ognuna:

Rete	IP iniziale	IP finale	Broadcast
x.x.x.0	x.x.x.1	x.x.x.62	x.x.x.63
x.x.x.64	x.x.x.65	x.x.x.126	x.x.x.127
x.x.x.128	x.x.x.129	x.x.x.190	x.x.x.191
x.x.x.192	x.x.x.193	x.x.x.254	x.x.x.255

Maschera di rete a 27 bit, pari a 255.255.255.224, per otto sottoreti con 30 nodi ognuna:

```
rrrrrrrr, rrrrrrrr, rrrrrrrr, ssshhhh
```

Rete	IP iniziale	IP finale	Broadcast
x.x.x.0	x.x.x.1	x.x.x.30	x.x.x.31
x.x.x.32	x.x.x.33	x.x.x.62	x.x.x.63
x.x.x.64	x.x.x.65	x.x.x.94	x.x.x.95
x.x.x.96	x.x.x.97	x.x.x.126	x.x.x.127
x.x.x.128	x.x.x.129	x.x.x.158	x.x.x.159
x.x.x.160	x.x.x.161	x.x.x.190	x.x.x.191
x.x.x.192	x.x.x.193	x.x.x.222	x.x.x.223
x.x.x.224	x.x.x.225	x.x.x.254	x.x.x.255

Maschera di rete a 28 bit, pari a 255.255.255.240, per 16 sottoreti con 14 nodi ognuna:

```
rrrrrrrr, rrrrrrrr, rrrrrrrr, sssshhhh
```

Rete	IP iniziale	IP finale	Broadcast
x.x.x.0	x.x.x.1	x.x.x.14	x.x.x.15
x.x.x.16	x.x.x.17	x.x.x.30	x.x.x.31
x.x.x.32	x.x.x.33	x.x.x.46	x.x.x.47
x.x.x.48	x.x.x.49	x.x.x.62	x.x.x.63
x.x.x.64	x.x.x.65	x.x.x.78	x.x.x.79
x.x.x.80	x.x.x.81	x.x.x.94	x.x.x.95
x.x.x.96	x.x.x.97	x.x.x.110	x.x.x.111
x.x.x.112	x.x.x.113	x.x.x.126	x.x.x.127
x.x.x.128	x.x.x.129	x.x.x.142	x.x.x.143
x.x.x.144	x.x.x.145	x.x.x.158	x.x.x.159
x.x.x.160	x.x.x.161	x.x.x.174	x.x.x.175
x.x.x.176	x.x.x.177	x.x.x.190	x.x.x.191
x.x.x.192	x.x.x.193	x.x.x.206	x.x.x.207
x.x.x.208	x.x.x.209	x.x.x.222	x.x.x.223
x.x.x.224	x.x.x.225	x.x.x.238	x.x.x.239
x.x.x.240	x.x.x.241	x.x.x.254	x.x.x.255

Maschera di rete a 29 bit, pari a 255.255.255.248, per 32 sottoreti con sei nodi ognuna:

*rrrrrrrr, rrrrrrrr, rrrrrrrr, ssssshhh*

Rete	IP iniziale	IP finale	Broadcast
x.x.x.0	x.x.x.1	x.x.x.6	x.x.x.7
x.x.x.8	x.x.x.9	x.x.x.14	x.x.x.15
x.x.x.16	x.x.x.17	x.x.x.22	x.x.x.23
x.x.x.24	x.x.x.25	x.x.x.30	x.x.x.31
x.x.x.32	x.x.x.33	x.x.x.38	x.x.x.39
x.x.x.40	x.x.x.41	x.x.x.46	x.x.x.47
x.x.x.48	x.x.x.49	x.x.x.54	x.x.x.55
x.x.x.56	x.x.x.57	x.x.x.62	x.x.x.63
x.x.x.64	x.x.x.65	x.x.x.70	x.x.x.71
x.x.x.72	x.x.x.73	x.x.x.78	x.x.x.79
x.x.x.80	x.x.x.81	x.x.x.86	x.x.x.87
x.x.x.88	x.x.x.89	x.x.x.94	x.x.x.95
x.x.x.96	x.x.x.97	x.x.x.102	x.x.x.103
x.x.x.104	x.x.x.105	x.x.x.110	x.x.x.111
x.x.x.112	x.x.x.113	x.x.x.118	x.x.x.119
x.x.x.120	x.x.x.121	x.x.x.126	x.x.x.127
x.x.x.128	x.x.x.129	x.x.x.134	x.x.x.135
x.x.x.136	x.x.x.137	x.x.x.142	x.x.x.143
x.x.x.144	x.x.x.145	x.x.x.150	x.x.x.151

x.x.x.152	x.x.x.153	x.x.x.158	x.x.x.159
x.x.x.160	x.x.x.161	x.x.x.166	x.x.x.167
x.x.x.168	x.x.x.169	x.x.x.174	x.x.x.175
x.x.x.176	x.x.x.177	x.x.x.182	x.x.x.183
x.x.x.184	x.x.x.185	x.x.x.190	x.x.x.191
x.x.x.192	x.x.x.193	x.x.x.198	x.x.x.199
x.x.x.200	x.x.x.201	x.x.x.206	x.x.x.207
x.x.x.208	x.x.x.209	x.x.x.214	x.x.x.215
x.x.x.216	x.x.x.217	x.x.x.222	x.x.x.223
x.x.x.224	x.x.x.225	x.x.x.230	x.x.x.231
x.x.x.232	x.x.x.233	x.x.x.238	x.x.x.239
x.x.x.240	x.x.x.241	x.x.x.246	x.x.x.247
x.x.x.248	x.x.x.249	x.x.x.254	x.x.x.255

### 246.3.7 Indirizzi di rete critici

Teoricamente, una volta stabilita la disponibilità di indirizzi, è possibile suddividere questo insieme in reti e sottoreti, secondo le esigenze, sfruttando al massimo gli intervalli. Purtroppo però, bisogna fare i conti con delle consuetudini che in certe situazioni si traducono in problemi difficili da comprendere. In altri termini, a meno di disporre di software preparato per questo, è meglio stare lontani dai punti limite.

Quando si divide un gruppo di indirizzi in diverse sottoreti, teoricamente, la porzione di indirizzo che serve a distinguere le reti non può essere utilizzata con tutti i bit a zero e nemmeno con tutti i bit a uno. Per esempio, disponendo degli indirizzi da 192.168.0.0 a 192.168.255.255, conviene evitare di predisporre la rete 192.168.0.0 con maschera 255.255.255.0 e la rete 192.168.255.0 con maschera 255.255.255.0; infatti, nel primo caso si rischia di interferire proprio con l'indirizzo di rete, mentre nel secondo con l'indirizzo broadcast.

Viene mostrata una tabella che mostra alcuni esempi di indirizzi di rete da evitare quando si usano gli indirizzi privati.

*Tabella 246.21. Esempi di indirizzi di sottoreti negli intervalli degli indirizzi privati, che possono creare problemi.*

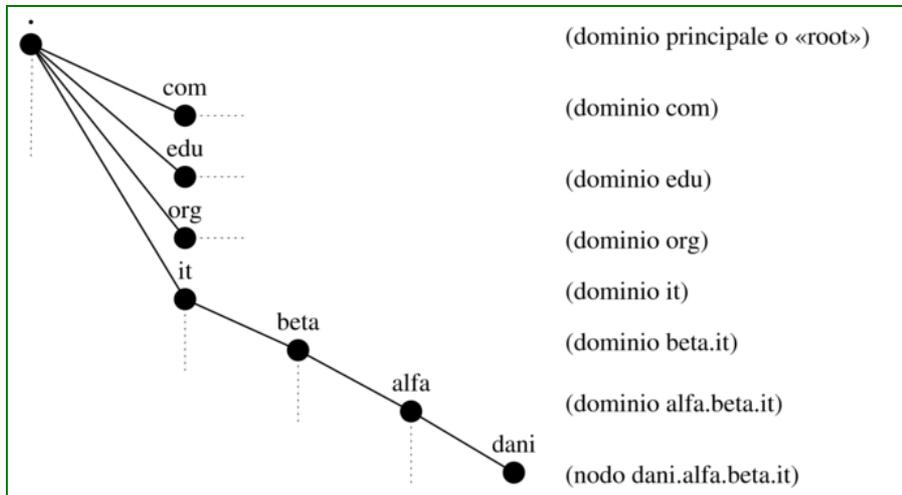
Indirizzo	Maschera	Descrizione
10.0.0.0	255.0.0.0	In questo caso si gestisce una sola rete privata con la maschera di rete predefinita e non dovrebbero esserci problemi.
10.0.0.0	255.255.0.0	Qui si fa una suddivisione in sottoreti e questa sottorete in particolare ha un indirizzo che può entrare in conflitto con l'indirizzo della rete complessiva, che sarebbe lo stesso.
10.255.0.0	255.255.0.0	Si fa una suddivisione in sottoreti, come nell'esempio precedente, ma si rischia di interferire con l'indirizzo broadcast della rete complessiva, che sarebbe lo stesso.
172.16.0.0	255.255.0.0	Si fa una suddivisione in sottoreti e questa sottorete in particolare ha un indirizzo che può entrare in conflitto con l'indirizzo della rete

		complessiva, che sarebbe lo stesso. Infatti, $16_{10}$ corrisponde a un otetto $00010000_2$ , dove gli ultimi quattro bit sono azzerati.
172.31.0.0	255.255.0.0	Si fa una suddivisione in sottoreti, come nell'esempio precedente, ma si rischia di interferire con l'indirizzo broadcast della rete complessiva, che sarebbe lo stesso. Infatti, $31_{10}$ corrisponde a un otetto $00011111_2$ , dove gli ultimi quattro bit sono tutti a uno.
192.168.0.0	255.255.255.0	Si fa una suddivisione in sottoreti e questa sottorete in particolare ha un indirizzo che può entrare in conflitto con l'indirizzo della rete complessiva, che sarebbe lo stesso.
192.168.255.0	255.255.0.0	Si fa una suddivisione in sottoreti, come nell'esempio precedente, ma si rischia di interferire con l'indirizzo broadcast della rete complessiva, che sarebbe lo stesso.

## 246.4 Nomi di dominio

La gestione diretta degli indirizzi IP è piuttosto faticosa dal punto di vista umano. Per questo motivo si preferisce associare un nome agli indirizzi numerici. Il sistema utilizzato attualmente è il DNS (*Domain name system*), ovvero il sistema dei nomi di dominio. Gli indirizzi della rete Internet sono organizzati ad albero in domini, sottodomini (altri sottodomini di livello inferiore, ecc.), fino ad arrivare a identificare il nodo desiderato.

Figura 246.22. Struttura dei nomi di dominio.



Non esiste una regola per stabilire quante debbano essere le suddivisioni, di conseguenza, di fronte a un nome del genere non si può sapere a priori se si tratta di un indirizzo finale, riferito a un nodo singolo, o a un gruppo di questi.

Con il termine **nome di dominio**, si può fare riferimento sia al nome completo di un nodo particolare, sia a una parte iniziale di questo, nel lato destro. Dipende dal contesto stabilire cosa si intende veramente. Per fare un esempio che dovrebbe essere più comprensibile, è come parlare di un percorso all'interno di un file system: può trattarsi di una directory, oppure può essere il percorso assoluto che identifica precisamente un file.

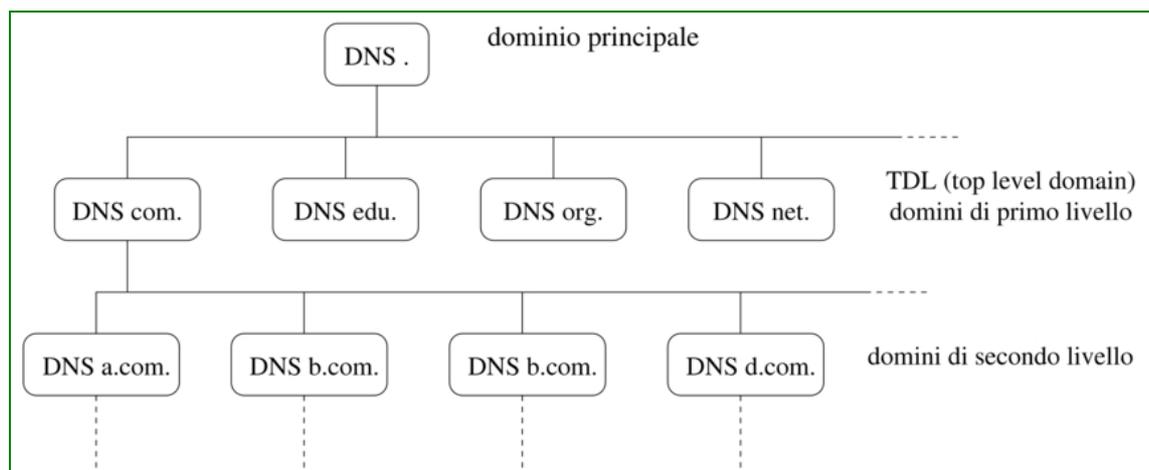
Spesso, all'interno della propria rete locale, è possibile identificare un nodo attraverso il solo nome finale (a sinistra), senza la parte iniziale del dominio di appartenenza. Per esempio, se la rete in cui si opera corrisponde al dominio `brot.dg`, il nodo `roggen` viene inteso essere `roggen.brot.dg`. Quando un nome di dominio contiene tutti gli elementi necessari a identificare un nodo, si parla precisamente di FQDN o *Fully qualified domain name*, quindi, `roggen.brot.dg` dell'esempio precedente è un FQDN.

Quando si realizza una rete locale con indirizzi IP non raggiungibili attraverso Internet, è opportuno abbinare nomi di dominio sicuramente inesistenti. Ciò aiuta anche a comprendere immediatamente che non si tratta di un dominio accessibile dall'esterno.

### 246.4.1 Servizio di risoluzione dei nomi di dominio

In un sistema di nomi di dominio (DNS), il problema più grande è quello di organizzare i *name server* ovvero i **servizi di risoluzione dei nomi** (servizi DNS). Ciò è attuato da nodi che si occupano di risolvere, ovvero trasformare, gli indirizzi mnemonici dei nomi di dominio in indirizzi numerici IP e viceversa. A livello del dominio principale (*root*), si trovano alcuni server che si occupano di fornire gli indirizzi per raggiungere i domini successivi, cioè `com`, `edu`, `org`, `net`, `it`,... A livello di questi domini ci sono alcuni server (ogni dominio ha i suoi) che si occupano di fornire gli indirizzi per raggiungere i domini inferiori, e così via, fino a raggiungere il nodo finale. Di conseguenza, un servizio di risoluzione dei nomi, per poter ottenere l'indirizzo di un nodo che si trova in un dominio al di fuori della sua portata, deve interpellare quelli del livello principale e mano a mano quelli di livello inferiore, fino a ottenere l'indirizzo cercato. Per determinare l'indirizzo IP di un nodo si rischia di dover accedere a una quantità di servizi di risoluzione dei nomi; pertanto, per ridurre il traffico di richieste, ognuno di questi è in grado di conservare autonomamente una certa quantità di indirizzi che sono stati richiesti nell'ultimo periodo.

Figura 246.23. Suddivisione delle competenze tra i vari servizi di risoluzione dei nomi.



In pratica, per poter utilizzare la notazione degli indirizzi suddivisa in domini, è necessario che il sistema locale sul quale si opera possa accedere al suo servizio di risoluzione dei nomi più vicino, oppure gestisca questo servizio per conto suo. In una rete locale privata composta da nodi che non sono raggiungibili dalla rete esterna (Internet), non dovrebbe essere necessario predisporre un servizio di risoluzione dei nomi; in questi casi è comunque indispensabile almeno il file `/etc/hosts` (270.2.1) compilato correttamente con gli indirizzi associati ai nomi completi dei vari nodi della rete locale.

## 246.5 Kernel Linux, configurazione per la rete

Per poter utilizzare i servizi di rete è necessario avere previsto questa gestione durante la configurazione del kernel. Per quanto riguarda GNU/Linux, si tratta principalmente di attivare la gestione della rete in generale e di attivare le particolari funzionalità necessarie per le attività che si intendono svolgere (sezione [72.2.14](#)).

Oltre alla gestione della rete, occorre anche pensare al tipo di hardware a disposizione; per questo si deve configurare la parte riguardante i dispositivi di rete.

## 246.6 Riferimenti

- Olaf Kirch, *NAG, The Linux Network Administrators' Guide*

<http://www.google.com/search?q=%22olaf+kirch%22+nag+%22the+linux+network+administrators+guide%22>

- Terry Dawson, *Linux NET-3-HOWTO*

<http://www.linux.org/docs/ldp/howto/HOWTO-INDEX/howtos.html>

- S. Gai, P. L. Montessoro, P. Nicoletti, *Reti locali: dal cablaggio all'internetworking*, UTET, edizione Scuola superiore G. Reiss Romoli, 1997
- Charles Hedrick, *TCP/IP introduction*, 1987

<http://www.iu.uib.no/~magnus/TCP.html>

- Mike Oliver, *TCP/IP Frequently Asked Questions*

<http://www.itprc.com/tcpipfaq/>

Appunti di informatica libera 2007.02 --- Copyright © 2000-2007 Daniele Giacomini --  
<daniele (ad) swlibero-org>