Networking

- Indirizzo IP
- Maschera di rete

Definizione di una rete IP: una classe di indirizzi IP accomunati dallo stesso prefisso (parte a sinistra dell'indirizzo). La lunghezza del prefisso è variabile e si deduce dalla netmask. Esempio:

Esempio 1

192.168.3.1/255.255.255.0		Rete di 256 indirizzi IP (24 bit), da 192.168.3.0 a 192.168.3.255.
192.168.3.0	**00000000**	Indirizzo riservato, indica la rete intera.
192.168.3.1	**00000001**	Primo indirizzo utile da assegnare ad un host.
...		...
192.168.3.254	**11111110**	Ultimo indirizzo utile da assegnare ad un host.
192.168.3.255	**11111111**	Indirizzo risevato detto di broadcast, usato per comunicare contemporaneamente con tutti gli host di questa rete.

Esempio 2

2.119.27.177/255.255.255.248		Rete di 8 indirzzi IP, netmask di 29 bit.
2.119.27.176	**10110 000**	Indirizzo riservato, indica la rete intera.
2.119.27.177	**10110 001**	Primo indirizzo utile.
...		...
2.119.27.182	**10110 110**	Ultimo indirizzo utile.
2.119.27.183	**10110 111**	Indirizzo di broadcast.

Come calcolare gli indirizzi di rete

Servizio on-line: http://www.subnet-calculator.com/cidr.php

Con è installato **`shorewall`**:

```
root@naxos:~# shorewall ipcalc 2.119.27.178/29
   CIDR=2.119.27.178/29
   NETMASK=255.255.255.248
   NETWORK=2.119.27.176
   BROADCAST=2.119.27.183
```

Indirizzi privati per reti locali

Alcuni classi di indirizzi IP sono riservati alle reti locali, quindi sono indirizzi che non sono raggiungibili direttamente su internet. Vedere RFC 1918.

Primo indirizzo	Ultimo indirizzo
10.0.0.0	10.255.255.255
172.16.0.0	172.31.255.255
192.168.0.0	192.168.255.255

Di solito **le reti private sono a 24 bit**, (del tipo 192.168.9.0/24), il limite è nel numero di **host presenti nella rete: max 254**.

Per reti con più di 254 host di solito si sceglie un indirizzo del tipo **10.x.0.0/16**. In questo caso si possono avere max 65534 host.

Comandi per debug

- traceroute
- tcpdump
- arp
- nmap

Visualizza gli **hop della rotta** verso una destinazione:

```
root@sysadmin:~# traceroute google.com
traceroute to google.com (74.125.232.115), 30 hops max, 60 byte packets
 1  naxos.rigacci.net (192.168.3.1)  0.748 ms  0.694 ms  0.681 ms
 2  static-213-205-53-76.clienti.tiscali.it (213.205.53.76)  45.260 ms
45.261 ms  53.365 ms
 3  static-213-205-28-66.clienti.tiscali.it (213.205.28.66)  53.363 ms
59.442 ms  59.441 ms
 4  static-213-205-56-113.clienti.tiscali.it (213.205.56.113)  63.310 ms
67.290 ms  77.903 ms
 5  94.32.128.145 (94.32.128.145)  77.898 ms  77.884 ms  86.433 ms
 6  ae2-300.mil20.ip4.tinet.net (77.67.94.37)  86.429 ms  92.412 ms  92.371
ms
 7  as15169.ip4.tinet.net (77.67.72.254)  101.671 ms as15169.ip4.tinet.net
(77.67.72.250)  63.319 ms  63.289 ms
 8  209.85.249.54 (209.85.249.54)  55.072 ms  62.060 ms  56.832 ms
 9  72.14.232.63 (72.14.232.63)  63.675 ms  51.699 ms  51.770 ms
10  74.125.232.115 (74.125.232.115)  59.892 ms  59.894 ms  67.763 ms
```

Visualizza il **traffico su una interfaccia di rete**, es. monitorizzo un ping:

```
tcpdump
root@sysadmin:~# tcpdump -i eth0 -n 'not port 22'
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 65535 bytes
15:31:45.455837 ARP, Request who-has 192.168.3.112 tell 192.168.3.113,
length 28
15:31:45.456525 ARP, Reply 192.168.3.112 is-at 00:17:08:49:6d:41, length 46
```

```
15:31:45.456537 IP 192.168.3.113 > 192.168.3.112: ICMP echo request, id
1568, seq 1, length 64
15:31:45.457297 IP 192.168.3.112 > 192.168.3.113: ICMP echo reply, id 1568,
seq 1, length 64
15:31:46.454605 IP 192.168.3.113 > 192.168.3.112: ICMP echo request, id
1568, seq 2, length 64
```

Visualizza la **tabella di arp** (associazione tra indirizzi IP e indirizzi MAC Ethernet):

```
root@sysadmin:~# arp -n
Address                  HWtype  HWaddress           Flags Mask
Iface
192.168.3.1              ether   00:25:86:e5:fb:2e   C
eth0
192.168.3.32             ether   00:18:84:20:a3:28   C
eth0
```

Visualizza le **porte aperte** (servizi attivi) su un host remoto:

```
root@sysadmin:~# nmap 2.119.27.178

Starting Nmap 5.21 ( http://nmap.org ) at 2011-04-12 16:17 CEST
Nmap scan report for host178-27-static.119-2-b.business.telecomitalia.it
(2.119.27.178)
Host is up (0.20s latency).
Not shown: 999 filtered ports
PORT   STATE SERVICE
22/tcp open  ssh

Nmap done: 1 IP address (1 host up) scanned in 22.91 seconds
```

Controlla lo stato di un range di porte:

```
root@sysadmin:~# nmap -p 10-1196 2.119.27.178

Starting Nmap 5.21 ( http://nmap.org ) at 2011-04-12 16:41 CEST
Nmap scan report for host178-27-static.119-2-b.business.telecomitalia.it
(2.119.27.178)
Host is up (0.22s latency).
Not shown: 1185 filtered ports
PORT     STATE SERVICE
22/tcp   open  ssh
1194/tcp open  unknown

Nmap done: 1 IP address (1 host up) scanned in 20.68 seconds
```