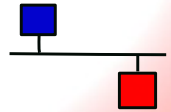
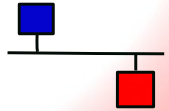
Hakerare la Rete

Piccoli consigli per iniziare a capire come i PC comunicano e cosa possono fare in rete



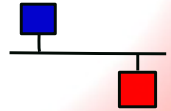
Scoprire i propri parametri di rete

- I miei indirizzi
  - ip address list
  - Ifconfig
- I router della mia rete
  - ip route list
  - route
- La magia dei nomi: il DNS
  - cat /etc/resolv.conf



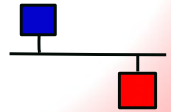
Anatomia di un indirizzo IPv4

- Dal comando `ip address list` abbiamo ottenuto
  `inet 192.168.100.100/24`
- Questo è l'indirizzo IP (o meglio l'indirizzo IPv4) della nostra macchina
- È composto da quattro numeri a tre cifre separati da un punto e da un numero a due cifre separato da una /
- I quattro numeri a tre cifre (ma potrebbero essere anche due o una sola) rappresentano ciascuno il valore di **uno dei byte** dell'indirizzo e possono andare da 0 a 255
- Un indirizzo IP è un numero a 32 bit.
- Questo indirizzo indica una singola macchina in una particolare rete, quindi va diviso in due parti:
  - L'indirizzo di rete
  - L'indirizzo della macchina nella rete
- Queste due parti non sono sempre della stessa dimensione, quindi si indica il **/24** che indica che l'indirizzo della rete occupa i **primi 24 bit** (tre byte) dell'indirizzo IP
- Di conseguenza l'indirizzo della macchina nella rete occupa i **restanti 8 bit**
- L'indirizzo della **rete** è **192.168.100**
- L'indirizzo della **macchina** nella rete è **100**
- Più avanti vedremo indirizzi divisi in maniera diversa.



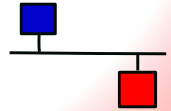
Modo alternativo

- Se invece del comando ip address list utilizzassimo il comando ifconfig, non più supportato dai nuovi sistemi operativi, l'informazione che otteniamo è:
  `inet 192.168.100.10  netmask 255.255.255.0`
- Quindi ci vengono proposti due gruppi, con la stessa forma. Il primo è sempre l'indirizzo IPv4 a 32 bit espresso in forma puntata
- Il secondo, chiamato netmask a sempre il compito di indicare la parte dell'indirizzo della rete.
- Se il numero nella maschera è 255, allora il numero corrispondente dell'indirizzo sarà riferito alla rete, se è 0, allora si riferirà alla macchina:
  192.168.100. *10*
  255.255.255. *0*
- La parte in **grassetto** è l'indirizzo di **rete**, quella in *corsivo*, l'indirizzo della **macchina**.
- Naturalmente ho ipotizzato che gli indirizzi di rete e di macchina occupassero sempre dei byte interi, ma questo non è sempre vero, in questo caso troveremo dei numeri diversi da 0 e 255.



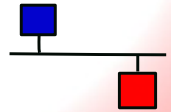
Verifica di connettività locale

- Proviamo ora a vedere se riusciamo a comunicare con le macchine della stessa nostra rete.
- Queste macchine dovranno condividere gli stessi **primi tre byte**, visto che questa è una rete ***/24***
- Potremo usare i due comandi:
  `ping 192.168.100.10`
  `ping 192.168.100.1`
- Per **interrompere** il comando ping, si userà la combinazione di tasti **Ctrl+C** (**^C**)
- Per contattare l' altra macchina che fa parte della mia installazione ma non della mia LAN, devo verificare la configurazione di un router



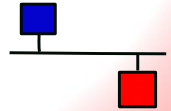
Il router

- Le macchine della mia **rete locale** sono tutte quelle connesse allo **stesso switch** o alla **stessa rete Wireless**.
- Se voglio connettermi a macchine di **reti diverse**, appartenenti alla mia installazione oppure in Internet, devo inviare i dati ad un **router**, che potrà instradare i miei dati verso la rete giusta.



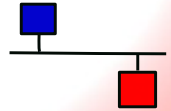
La configurazione delle rotte

- Per vedere come sono configurate le rotte abbiamo due comandi, come al solito il vecchio ed il nuovo:
  ```
  ip route list
  route
  ```
- In entrambi i casi troviamo due reti:
  - **default**, che utilizza come router (**gateway**) **192.168.100.1** (o LEDE.lan)
  - **192.168.100.0/24** (o 192.168.100.0 netmask 255.255.255.0) che usa come router **0.0.0.0**, quindi non ha router ed è **direttamente connessa** alla scheda



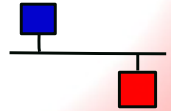
Connessioni fuori dalla nostra lan

- Ora possiamo anche controllare la connettività con le macchine fuori dalla nostra rete.
- Controlleremo per prima cosa se il default gateway è raggiungibile:
  `ping 192.168.100.1`
- Se lo è proviamo a contattare la macchina sull'altra rete:
  `ping 172.16.10.10`
- Per finire proviamo a contattare un server esterno. Useremo un server noto con u indirizzo facile:
  `ping 1.1.1.1`



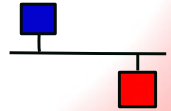
Ma che strada faccio

- Ora, scoperto che posso raggiungere una serie di macchine, vediamo che strada fanno i nostri pacchetti per raggiungere queste destinazioni.
- Per far questo potremo usare il comando traceroute:
  `traceroute 192.168.100.10`
  `traceroute 172.16.10.10`
  `traceroute 1.1.1.1`
- Scopro che:
- 192.168.100.10 viene raggiunto immediatamente
- Per `172.16.10.10 si deve attraversare il solo route LEDE.lan`
- `Per raggiungere 1.1.1.1 deve attraversare 13 o 14 router`



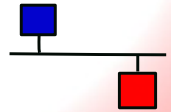
Belli gli IP, ma e i nomi?

- Con questo abbiamo verificato la cnnettività della nostra macchina.
- Se vogliamo però utilizzare i nomi dei siti, ci serve collegarsi ad un servizio esterno: la rete dei DNS (o Domain Name System)
- Ci basterà essere connesso ad uno dei server che ne fanno parte per poter ottenere informazioni su tutti i nomi di Internet.
- Le informazioni su questo server le troviamo nelfile /etc/resolv.conf (almeno nella configurazione tradizionale, senza Systemd che gestisce la cosa). Per visualizzarlo potremo dare il comando:
  `cat /etc /resolv.conf`
- La riga importante di questo file è:
  `nameserver 192.160.100.1`
- Che indica il server utilizzato per risolvere i nomi, vale a dire per dirci a che indirizzo corrisponde un certo nome
- Possiamo provarlo cercando il nome della macchina su cui siamo: dell:
  `host dell`
- Il DNS offre anche il servizio contrario: dall'IP risale al nome della macchina:
  `host 192.168.100.100`



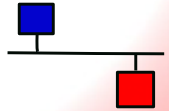
Cominciamo le vere ricerche

- Ok, fino a qui la teoria e la verifica di cose che sappiamo.
- Proviamo ora a fare delle ricerche per vedere cosa contiene la nostra rete.
- Useremo il comando nmap che fa una serie di prove.
- Per incominciare, chiediamo ad nmap che macchine ci sono nella nostra rete:
  `nmap 192.168.100.1-254`
- Ci mette un po' di tempo, perché deve provare tutti gli indirizzi della nostra rete, dal 192.168.100.1 al 192.168.100.254
- Trova almeno tre macchine, e ne descrive i servizi di base, oltre al nome:
  - LEDE.lan (192.168.100.1 – il router) con i servizi ssh, domain, http
  - raspberrymy.lan (192.168.100.10) con i servizi ssh ed http
  - dell.lan (192.168.100.100) con i servizi daytime, ssh ed http



Vediamo che macchina è

- Con nmap possiamo fare anche delle ricerche approfondite
- Potremmo dare il comando
  nmap -A -T4 192.168.100.10
  - -A abilita il riconoscimento del sistema operativo
  - -T2 analisi “educata”, cerca di scoprire i server ce offroo i servizi, ma senza fare richieste troppo “strane”, vale a dire analizzando le risposte normali che il servizio da
- Scopriremmo che:
  - Il server SSH è un OpenSSH versione 7.41 appartenete a raspbian
  - Il server HTTP è un Apache versione 2.4.25 sempre apparenente a raspbian
  - Il Mac Address della scheda di rete indica che fa parte di un Raspberry Pi
  - Il sistema operativo è un Linux con kernel della versione 3
- Naturalmente nmap ci dice il modello della scheda di rete solo per le macchine nella nostra LAN, per le quali può individuare l’indirizzo MAC della scheda di rete.
- Se facciamo l’nmap su 172.16.10.10 questa informazione non ci viene data.



Una piccola ricerca

- Possiamo scoprire su che provider girano alcuni siti?
- Grazie al Reverse DNS, si.
- Proviamo a vedere su che fornitore gira **www.interflora.it**
- Per prima cosa, con il comando host troveremo il suo indirizzo IP
- Ora cercheremo, sempre con host, l'indirizzo IP per scoprire il nome.
- Il nome dell'host non è www.interflora.com, ma quello del server su cui gira