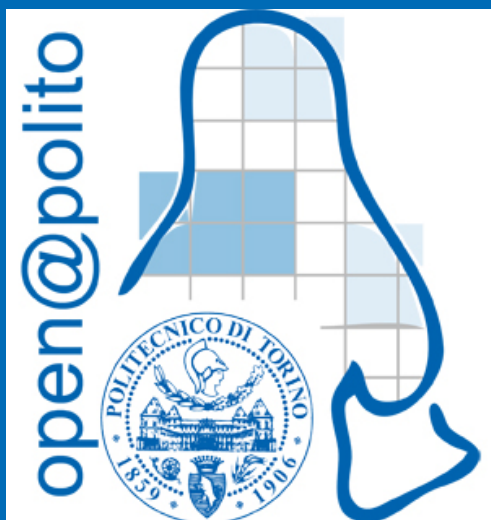




Con il supporto di



# Networking

Fondamenti

Di @oirasor

---

# Unix Philosophy

[https://en.wikipedia.org/wiki/Unix\\_philosophy](https://en.wikipedia.org/wiki/Unix_philosophy)

**Make each program do one thing well**

Seguendo questa filosofia si sono affermati alcuni comandi:

[https://en.wikipedia.org/wiki/List\\_of\\_Unix\\_commands](https://en.wikipedia.org/wiki/List_of_Unix_commands)

[https://en.wikipedia.org/wiki/List\\_of\\_GNU\\_Core\\_Uutilities\\_commands](https://en.wikipedia.org/wiki/List_of_GNU_Core_Uutilities_commands)

Liste utili per approfondire in autonomia aspetti non trattati in questo corso

# Networking

In principio fu **net-tools**  
`sudo apt install net-tools`

Un giorno comparve **iproute2** (since 1999 for Linux 2.2)  
<https://en.wikipedia.org/wiki/Iproute2>

<https://it.wikipedia.org/wiki/Iproute2>

**Make each program do one thing well?**

# Quadro Sinottico

net-tools	iproute2	Gestisce
ifconfig	ip addr, ip link, ip -s	Indirizzo e configurazione del link
route	ip route	Tabelle di routing
arp	ip neigh	Tabelle degli apparati vicini (tabella ARP per IPv4)
iptunnel	ip tunnel	Tunnel
nameif, ifrename	ip link set name	Rename del link
ipmaddr	ip maddr	Multicast
netstat	ip -s, ss, ip route	Statistiche di rete

# Bignami?

- filetype:pdf cheatsheet ...
- filetype:pdf cheatsheet ip

[https://access.redhat.com/sites/default/files/attachments/rh\\_ip\\_command\\_cheatsheet\\_1214\\_jcs\\_print.pdf](https://access.redhat.com/sites/default/files/attachments/rh_ip_command_cheatsheet_1214_jcs_print.pdf)

- filetype:pdf cheatsheet linux

<https://images.linuxide.com/linux-cheat-sheet.pdf>

- filetype:pdf cheatsheet shell scripting

<http://dcjtech.info/wp-content/uploads/2015/12/Shell-Scripting.pdf>

# E la rete sia

```
ifconfig eth0 192.168.1.100  
route add default gw 192.168.1.1  
vim /etc/resolv.conf  
nameserver 208.67.222.222  
nameserver 208.67.220.220
```

```
ip addr add 192.168.1.100/24 dev eth0  
ip route add default via 192.168.1.1  
vim /etc/resolv.conf  
nameserver 208.67.222.222  
nameserver 208.67.220.220
```

Oppure semplicemente  
dhclient eth0  
**se disponibile il DHCP**

# Altri comandi in ordine sparso

- hostname
- ping
- tracepath / traceroute
- dig / nslookup
- whois
- netstat
- nmap
- tcpdump
- nc /netcat
- wget
- telnet (es. telnet freechess.org)
- ssh
- Protocollo SMB (es. smbclient)
- ...

# TCP vs UDP

TCP



UDP



- Reliable
- Connection-oriented
- Windowing & Retransmission
- Segment sequencing
- Acknowledge segments

- Unreliable
- Connectionless
- No windowing or retransmission
- No sequencing
- No acknowledgment



# nc

- E' un tool che permette a due host di comunicare, utilissimo per
  - Effettuare port scanning
  - creare una connessione con protocollo TCP e UDP
  - Volendo, anche trasferire file
  - Bonus? Simulare una backdoor

# Porte comuni

PORT NUMBER	USAGE	DESCRIPTION
20/21	FTP Data and FTP Control	During a FTP session, data flows through Port 20 whilst control information flows down Port 21.
22	Secure Shell (SSH)	SSH Provides secure access to devices over a tcp/ip network. A secure replacement to telnet
23	Telnet	Telnet provides access to devices over a network. However, unlike SSH, provides no security.
25	SMTP	SMTP is used to transfer mail between email servers.
53	DNS	DNS (Domain Name System) is used to translate domain names into IP addresses.
67/68	DHCP	DHCP (Dynamic Host Configuration Protocol) is used to provide IP addresses to devices that do not have a static IP address.
69	TFTP	Typically used by devices for installing/upgrading software.
80	HTTP	HTTP (Hyper Text Transfer Protocol) is the main protocol used by browsers.
110	POP3	Post Office Protocol version 3 is used by mail client programs for the transferring of mail to a server.
123	NTP	NTP (Network Time Protocol) used for time synchronization of networked devices.
143	IMAP	Internet Message Access Protocol - Alternative to POP3.
161/162	SNMP	SNMP (Simple Network management Protocol) often used for monitoring network equipment.
179	BGP	BGP (Border Gateway Protocol), used for managing very large routing tables.
389	LDAP	LDAP (Lightweight Directory Access Protocol.
443	HTTPS	HTTPS (Hyper Text Transfer Protocol Secure), HTTP over SSL/TLS.

# ssh & scp

- Sono due tool molto utilizzati per interagire con un server
  - ssh permette di connettersi ad un <host> dato un nome utente <user>
    - ♦ `ssh <user>@<host>` o `ssh -l <user> -h <host>` (richiede la password)
  - scp serve per copiare file tra due host.
    - ♦ `scp <user>@<host> ~/file.txt .` (copio il file txt dalla home remota alla mia \$PWD)

Quest'opera, per volontà degli autori, è rilasciata sotto la disciplina della seguente licenza

**Creative Commons Public License**  
**Attribuzione - Condividi allo stesso modo 4.0 Internazionale (CC BY-SA 4.0)**

**Tu sei libero**



**Condividere** — riprodurre, distribuire, comunicare al pubblico, esporre in pubblico, rappresentare, eseguire e recitare questo materiale con qualsiasi mezzo e formato



**Modificare** — remixare, trasformare il materiale e basarti su di esso per le tue opere per qualsiasi fine, anche commerciale.

Il licenziante non può revocare questi diritti fintanto che tu rispetti i termini della licenza.

**Alle seguenti condizioni**



**Attribuzione** — Devi riconoscere una menzione di paternità adeguata, fornire un link alla licenza e indicare se sono state effettuate delle modifiche. Puoi fare ciò in qualsiasi maniera ragionevole possibile, ma non con modalità tali da suggerire che il licenziante avalli te o il tuo utilizzo del materiale.



**Stessa Licenza** — Se remixi, trasformi il materiale o ti basi su di esso, devi distribuire i tuoi contributi con la stessa licenza del materiale originario.

**Divieto di restrizioni aggiuntive** — Non puoi applicare termini legali o misure tecnologiche che impongano ad altri soggetti dei vincoli giuridici su quanto la licenza consente loro di fare

Questo è un riassunto in linguaggio accessibile a tutti del codice legale (la licenza integrale) che è disponibile alla pagina web

<https://creativecommons.org/licenses/by-sa/4.0/legalcode.it>