Alcuni strumenti di uso comune per l'analisi dello stato del sistema

Verificare con i seguenti comandi lo stato del sistema
(consultare il man in linea `man nomecomando`*):*

file system:

- **df** mostra lo stato di occupazione dei dischi
- **du** mostra la dimensione dei file e delle directory in una parte di file system

gestione processi:

- **ps** process status, fornisce una descrizione dei processi in esecuzione in una macchina; provare le opzioni -aux (Unix BSD) e -ef (System V)
- **kill -segnale pid** per mandare un segnale al processo pid (per esempio `kill -9 pid` uccide il processo con l'identificatore `pid`)

file di sistema nel direttorio /etc

i file di inizializzazione: rc, rc.local
altri file:

services (allegato in ultima pagina)
password
hosts
network
hosts.equiv
fstab
protocol
inetd.conf

nome dell'host: **hostname**
nome del dominio: **domainname**

Strumenti di rete

ftp (porte 20-21)

provare il site anonymous su didahp1 (dare come username anonymous e come passwd il proprio indirizzo di e-mail)
collegarsi ed esaminare l'ambiente di lavoro e le possibilità a disposizione

In particolare tentare un collegamento usando il flag -d
ftp -d lia01
che consente di visualizzare tutti i messaggi di accordo tra il cliente ed il servitore
oppure
ftp
e richiedere l'help
?

Si provino le opzioni debug, hash, etc.
Si usi il nome di file **-** per visualizzare su video, o il nome con inizio | per invocare uno shell:
get filename -
get filename "| more"

telnet (porta 23)

usare una sessione di telnet con possibilità di vedere tutte le opzioni

telnet
telnet> **?**
telnet> **toggle options**
telnet> **open deis33**

Si provi il telnet su una porta specifica, usando il servitore di echo o di discard, o di time:
telnet nomenodo daytime
telnet nomenodo echo
I servitori di telnet come echo o discard continuano a lavorare sull'input, ma si possono interrompere usando il **<CTRL>**]

rlogin

esaminare tutti i file rilevanti

/etc/hosts.equiv
~utente/.rhosts per l'utente corrente

Si verifichino i processi creati e l'esistenza di demoni per i singoli strumenti
Si provino inoltre i comandi: rcp, rsh, rup, ruptime, rusers, rwho, ...

mail (porta 25)

il demone di mail si chiama **sendmail**
ci sono molti lettori: **Mail, mail,** oppure **elm** su alcune workstation

se si manda un messaggio al lettore con -v
si invoca il demone in modo verboso per ottenere una stampa in chiaro
dei diversi passaggi del messaggio

WWW (porta 80)

possibilità di navigare in Internet utilizzando Netscape. Tale browser è utilizzabile anche per i servizi di **news** e **gopher**.

ping

si inviano una serie di messaggi ICMP al nodo specificato: si riportano le statistiche dei diversi messaggi
ping -svRlr nomehost dimensionepacchetto numeropacchetti

- **-s** ogni secondo
- **-v** verboso
- **-R** memorizza il route (record route)
- **-l** loose route
- **-r** invio diretto

finger (porta 79)

si richiedono informazioni su un nodo in relazione ad uno o più utenti
finger nomeutente@nomehost

arp

E’ possibile esaminare la tabella locale di arp attraverso il comando **arp**

arp -a

stampa la intera tabella delle corrispondenze arp (address resolution protocol) stabilite dalle comunicazioni.

inetd

Verificare la presenza del demone di inetd e vedere quali sono i servizi gestiti da ogni singola macchina.
Inoltre, si veda quali sono i processi generati per ogni singola azione applicativa.
Si esamini il file inetd.conf.

nslookup

Il comando consente di interrogare esplicitamente un name server.
Entrare nell’ambiente e richiedere i comandi disponibili

nslookup

nomelogico (risposta: indirizzo fisico)
ls nomedominio >filetemporaneo

(es. deis38.deis.unibo.it
ls deis.unibo.it
ls cineca.it)

per la corrispondenza inversa: da fisico a logico

set q=ptr
nomefisicoinvertito**.in-addr.arpa.**

(es. 137.204.57.38 => ***38.57.204.137.in-addr.arpa***)

netstat

analisi dello stato della rete

netstat

si provino le diverse opzioni, in particolare

- **-r** tabelle di routing
- **-a** comunicazione generale
- **-s** statistiche sui dati dei vari protocolli
- **-m** buffer
- **-n** visualizza gli indirizzi IP

Si esamini con attenzione la specifica delle tabelle di routing

netstat -r

Si notino: i **flag**: U per up, G per gateway, H per host, D per redirect.

netstat -A

Le connessioni in atto, sia tcp, sia udp.

netstat -a

anche lo stato delle socket

ifconfig

analisi della configurazione dell'interfaccia di rete (maschera di rete etc.)
ifconfig -a

traceroute

/usr/local/bin/**traceroute** traccia il percorso di routing verso l'host
Si noti che usa messaggi limitandone il numero di hop e si basa sulle indicazioni ottenute in risposta (errori ICMP).
Per andare oltre, sfrutta il source routing in IP.

rpcinfo

Strumento di analisi della tabella di port map di un nodo specifico.
Sono possibili invocazioni molto differenziate a secondo delle opzioni: si cerchi l'opzione per listare l'intero contenuto della tabella, per ritrovare la corrispondenza ad un programma e versione specificati.

rpcinfo -p nomehost
estrae l'intera tabella dinamica
rpcinfo [-n #porta] -u nomehost programma [versione]
rpcinfo [-n #porta] -t nomehost programma [versione]
verifica la presenza di un servizio per un nodo specificato e per un programma specificato, dando o meno la porta relativa e la versione
due tipi di protocollo, t per tcp ed u per udp
rpcinfo -b programma versione
invia in ***modo broadcast*** una procedura nulla per ogni nodo

Si noti che programma può essere espresso come numero fisico (100000 per il portmapper) o come nome logico (registrato nel file /etc/rpc locale e traslato automaticamente).

Esempio: si provino
rpcinfo -b spray (o 100012) 1
rpcinfo -b rusers (o 100012) 1
che definiscono comandi che non terminano ma continuano a riportare i messaggi di risposta.

File /etc/services

```
# Network services, Internet style
tcpmux          1/tcp                   # rfc-1078
echo            7/tcp
echo            7/udp
discard         9/tcp           sink null
discard         9/udp           sink null
systat          11/tcp          users
daytime         13/tcp
daytime         13/udp
netstat         15/tcp
ftp-data        20/tcp
ftp             21/tcp
telnet          23/tcp
smtp            25/tcp          mail
time            37/tcp          timserver
time            37/udp          timserver
name            42/udp          nameserver
whois           43/tcp          nicname         # usually to sri-nic
domain          53/udp
domain          53/tcp
http            80/tcp
hostnames       101/tcp         hostname        # usually to sri-nic
pop-3           110/tcp                 # Post Office version 3
sunrpc          111/udp                 # portmapper
sunrpc          111/tcp
#
# Host specific functions
tftp            69/udp
finger          79/tcp
x400            103/tcp                 # ISO Mail
uucp-path       117/tcp
nntp            119/tcp         usenet  # Network News Transfer
ntp             123/tcp                 # Network Time Protocol
NeWS            144/tcp         news    # Window System
# UNIX specific services
# these are NOT officially assigned
login           513/tcp
shell           514/tcp         cmd     # no passwords used
printer         515/tcp         spooler # line printer spooler
uucp            540/tcp         uucpd   # uucp daemon
who             513/udp         whod
syslog          514/udp
dyland          515/udp
talk            517/udp
route           520/udp         router routed
```