

Prove di servizi e strumenti - livello TCP

È disponibili un server accessibile dai vari laboratori:

Nome di DNS: retila-corradi.corsi.labx

Ogni studente accede con la propria utenza di Facoltà
(la stessa utilizzata in lab2 e lab3, vedere “Calcolo dello username”
nel sito <http://infox.ing.unibo.it/>)

Accesso tramite SSh (porta 22)

In particolare è possibile effettuare login remoto sicuro sul server invocando da shell il comando

```
ssh nomeutente@retila-corradi.corsi.labx  
Password: propriaPassword
```

A questo punto tutti i comandi lanciati vengono eseguiti sulla macchina remota (**retila-corradi.corsi.labx**).

In particolare, **retila-corradi.corsi.labx** mette a disposizione degli utenti che si collegano **dalla macchina locale** (*invocazione su localhost*) i server:

telnet Accessibile **solo in locale** con utenza:

Username: retila
Password: retila

ftp Accessibile **solo in locale** con la stessa utenza

Tutti gli altri comandi possono invece essere testati **direttamente** con la shell disponibile dal proprio ambiente di lavoro Linux **in lab2 e lab3**

Strumenti e servizi applicativi

ftp (porte 20-21)

In particolare tentare un collegamento usando il flag -d

```
ftp -d nomeserver
```

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>]

Provare anche i comandi di rete...

hostname identità del nodo corrente

ifconfig esamina l'interfaccia con la rete

arp accesso alla cache arp

Visualizza e modifica la tabella di traduzione

indirizzo IP-indirizzo fisico usata dal protocollo di risoluzione.

```
ARP -s ind_inet ind_eth [ind_if]
```

```
ARP -d ind_inet [ind_if]
```

```
ARP -a [ind_inet] [-N ind_if]
```

-a Visualizza le voci ARP correnti prendendole dai dati del

protocollo. Se viene specificato `ind_inet`, sono visualizzati solo gli indirizzi IP e fisico del computer specificato. Se più di un'interfaccia di rete usa ARP, vengono visualizzate le voci di ogni tabella ARP.

-g Analogo a **-a**.

ind_inet Specifica un indirizzo internet.

-N ind_if Visualizza le voci ARP per l'interfaccia di rete specificata

da `ind_if`.

-d Elimina l'host specificato da `ind_inet`.

-s Aggiunge l'host e associa l'indirizzo internet `ind_inet` con l'indirizzo fisico `ind_eth`. L'indirizzo fisico è un numero composto da 6 byte esadecimali separati da un trattino.

La voce è permanente.

ind_eth Specifica un indirizzo fisico.

ind_if Se presente, specifica l'indirizzo internet dell'interfaccia

la cui tabella di traduzione deve essere modificata. Se non presente, viene assunta la prima interfaccia utilizzabile.

netstat stato locale TCP

-a comunicazione

-i statistica

-r tabelle di routing

-s

-m buffer

-I monitoring

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

Visualizza le statistiche del protocollo e le connessioni di rete TCP/IP

correnti.

NETSTAT [-a] [-e] [-l] [-n] [-s] [-p proto] [-r] [intervallo]

-a Visualizza tutte le connessioni e le porte di ascolto.

(Le connessioni del server non vengono normalmente visualizzate).

-e Visualizza le statistiche Ethernet. Queste possono essere combinate con l'opzione -s.

-n Visualizza indirizzi e numeri di porta in forma numerica.

-p proto Visualizza le connessioni per il protocollo definito da proto;

proto può essere tcp o udp. Se utilizzato con l'opzione -s per visualizzare le statistiche per protocollo, proto può essere tcp, udp o ip.

-r Visualizza il contenuto della tabella di routing.

-s Visualizza le statistiche per protocollo. Per impostazione predefinita, le statistiche sono visualizzate per TCP, UDP e IP; l'opzione -p può essere utilizzata per specificare un sottinsieme dell'impostazione predefinita.

intervallo Rivisualizza le statistiche selezionate, interrompendo per un numero di secondi pari a intervallo tra ogni visualizzazione. Premere CTRL+C per fermare la visualizzazione delle statistiche. Se omesso, netstat stamperà le informazioni di configurazione correnti una sola volta.

ping invia pacchetti ICMP al nodo remoto

ping -svRlr nomehost dimensionepacchetto numeropacchetti

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

ping

Sintassi: `ping [-t] [-a] [-n numero] [-l lunghezza] [-f] [-i TTL] [-v TOS]`

`[-r numero] [-s numero] [[-j host-list] | [-k host-list]]`

`[-w timeout] elenco-destinatione`

Opzioni:

- t** Ping eseguito sull'host specificato finché non viene interrotto.
 - a** Risolve gli indirizzi in nomi host.
 - n numero** Invia numero di richieste di eco.
 - l lunghezza** Invia dimensione buffer.
 - f** Imposta il flag Non frammentare nel pacchetto.
 - i TTL** Vita pacchetto.
 - v TOS** Tipo di servizio.
 - r count** Registra route per il conteggio dei punti di passaggio.
 - s count** Marca orario per il conteggio dei punti di passaggio.
 - j host-list** Libera route di origine lungo l'elenco host.
 - k host-list** Restringe route di origine lungo l'elenco host.
 - w timeout** Intervallo attesa (in millisecondi) per ogni risposta.
-

traceroute invio di messaggi fornendo informazioni sul routing (uso di messaggi con TTL crescenti e ICMP)

Sintassi Possibile:

```
tracert [-d] [-h maximum_hops] [-j host-list] [-w timeout]  
nome_destinazione
```

Opzioni:

-d Non risolve gli indirizzi in nome host.

-h maximum_hops Numero massimo di punti di passaggio per
ricercare

la destinazione.

-j host-list Libera route di origine lungo l'elenco host.

-w timeout Intervallo di attesa in millisecondi per ogni
risposta.

nslookup ambiente di accesso a servizi DNS

nslookup

> ?

Comandi: (gli identificatori sono indicati in lettere maiuscole,
[] significa opzionale)

NOME - stampa info sul NOME del host/dominio NOME usando il
server predefinito

NOME1 NOME2 - come sopra ma usando NOME2 come server

help or ? - stampa informazioni su comandi comuni

set OPZIONE - imposta una opzione

all - stampa opzioni, server corrente e host

[no]debug - stampa informazioni di debugging

[no]d2 - stampa informazioni dettagliate di debugging

[no]defname - aggiungi nome dominio ad ogni query

[no]recurse - per risposte ricorsive alla query

[no]search - usa elenco ricerca dominio

[no]vc - usa sempre un circuito virtuale

domain=NOME - imposta il NOME predefinito del dominio

srchlist=N1[/N2/.../N6]

- imposta dominio a N1 e la lista di ricerca a N1,N2, ecc.

root=NOME - imposta server principale a NOME

retry=X - imposta numero di tentativi a X

timeout=X - imposta intervallo iniziale di scadenza a X secondi

type=X

- imposta tipo query, (es. A,ANY,CNAME,MX,NS,PTR,SOA,SRV)

querytype=X - come per type

class=X - imposta la classe della query (es. IN (Internet), ANY)

[no]msxfr - usa Microsoft fast zone transfer

ixfrver=X - versione corrente da utilizzare nelle richieste di transfer IXFR

server NOME

- imposta server predefinito a NOME, utilizzando il server predefinito corrente

lserver NOME

- imposta server predefinito a NOME, utilizzando il server iniziale

finger [UTENTE] - usa finger per il NOME opzionale all'host corrente

root - imposta il server predefinito corrente alla root

ls [opt] DOMINIO [> FILE]

- elenca indirizzi nel DOMINIO (opzionale: output a FILE)

-a - elenca nomi canonici e alias

-d - elenca tutti i record

-t TIPO - elenca record del tipo indicato (es. A,CNAME,MX,NS,PTR ecc.)

view FILE - ordina un file di output "ls" e visualizza con pg

exit - esce dal programma

comandi relativo ad RPC

rpcinfo informazioni sul port mapper

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) 2

che definiscono comandi che non terminano ma continuano a riportare i
messaggi di risposta.

nfsstat informazioni su NFS

NOTA

Alcuni dei comandi sopra indicati potrebbero trovarsi in direttori non inclusi nel proprio **PATH**, ad esempio:

- **/sbin, /usr/sbin, ...**

Per eseguire i comandi che si trovano in tali direttori, senza invocarli ogni volta con un percorso assoluto, bisogna aggiungere al proprio **PATH** i nomi dei direttori che li contengono.

Ad esempio, è possibile modificare nella propria **HOME** il file **".profile"** (creandolo se non esiste), inserendo una nuova linea dove aggiungiamo al **PATH** attuale il direttorio **/sbin**:

```
PATH=$PATH:/sbin  
export PATH
```