Introduzione a Linux

Modulo 5: come lo uso in rete?

Alessandro Brunengo
Mirko Corosu
INFN – Sezione di Genova

Parte I

Generalita' sul networking

Protocolli di rete

- Un protocollo di rete e' una serie di regole che permettono a piu' calcolatori interconnessi di comunicare tra loro
- Un protocollo di rete stabilisce regole che riguardano tutti gli aspetti della comunicazione, dalle specifiche elettriche dei segnali e delle interfaccie di rete, all'instradamento dei messaggi, alle regole di dialogo delle applicazioni

TCP/IP

- Esistono numerosi protocolli di rete (DECNET, NETBIOS, SNA, ...)
- Il protocollo di rete in assoluto piu' diffuso si chiama TCP/IP (Transmission Control Protocol/Internet Protocol) che viene utilizzato nella maggior parte delle connessioni in Internet
- Nel seguito parleremo di TCP/IP

Indirizzo IP

- Ogni calcolatore in rete deve avere un indirizzo univoco, per poter comunicare
- Un indirizzo IP e' costituito da quattro bytes (cioe' quattro numeri compresi tra 0 e 255), usualmente indicati in forma decimale e separati da punti:

10.254.23.6

Netmask

- L'indirizzo IP e' in realta' costituito da due parti:
  - una parte che identifica la rete a cui l'indirizzo appartiene
  - una parte che identifica l'host all'interno della sua rete
- Per identificare quale parte dell'indirizzo indica la rete e quale l'host su utilizza una maschera (netmask)

Netmask (cont.)

- La netmask ha lo stesso formato dell'indirizzo IP (4 bytes, rappresentati con decimali separati da punti)
- Il significato della netmask e'
  - se un bit della netmask vale 1, il corrispondente bit dell'indirizzo fa parte dell'indirizzo di rete
  - se un bit della netmask vale 0, il corrispondente bit dell'indirizzo fa parte dell'indirizzo di host

Netmask (cont.)

- Ne segue che un indirizzo IP e' completamente specificato se si definiscono l'indirizzo e la netmask
- Ad esempio, l'indirizzo:

  193.201.14.35 255.255.255.0

  specifica che il calcolatore appartiene alla rete 193.201.14.0, ed ha per host address 35

Default gateway

- La struttura del protocollo TCP/IP e' tale che un calcolatore sa come comunicare con host appartenenti alla sua stessa rete, ma non e' capace di cominicare con host appartenenti a reti diverse
- Per comunicare all'esterno della sua rete ci si serve un computer speciale (router o gateway) che sa come farlo
- Un calcolatore deve quindi sapere a chi inviare i messaggi destinati a calcolatori in reti diverse dalla sua (il default gateway)

Default gateway (cont.)

- Il default gateway deve avere un indirizzo sulla stessa rete del nostro calcolatore
- L'informazione del default gateway non puo' essere imparata dinamicamente, quindi va inserita in qualche modo nella configurazione del calcolatore (in genere a mano)

DNS (Domain Name System)

- Per facilitare le cose agli utenti umani dei calcolatori, si usa associare un nome alfanumerico all'indirizzo
- L'associazione normalmente e' univoca, e deve essere accessibile a tutti
- Il protocollo che si occupa di fornire le associazioni nome-indirizzo si chiama DNS

DNS (cont.)

- Il nome (TCP/IP) di un calcolatore e' costituito da diversi nomi separati da punti:

  www.google.it

- Tutto quanto segue il primo punto (google.it nel nostro esempio) si chiama dominio
- Quello che precede il primo punto si chiama nome (simple name) dell'host
- Il nome completo si chiama Fully Qualified Domain Name (FQDN)

DNS (cont.)

- In generale i sistemi operativi chiedono all'atto della installazione il nome della macchina
- Se si configura una interfaccia di rete, viene chiesto il nome del dominio
- Viene poi modificato automaticamente il nome della macchina unendo il nome al dominio

Configurazione della rete

- Esistono due modi per specificare la configurazione della rete:
  - configurazione statica; in questo caso si devono conoscere l'indirizzo, la netmask, l'indirizzo del default gateway, il nome ed il dominio di appartenenza; queste informazioni vanno sempre chieste al network administrator della rete a cui si connette il calcolatore
  - configurazione dinamica, via un protocollo che si chiama DHCP

DHCP

- Il DHCP (Dynamic Host Configuration Protocol) e' un protocollo che permette ad un host di inviare sulla sua interfaccia di rete la richiesta dei parametri di configurazione
- Deve esserci un DHCP server che risponda comunicando tutti i parametri necessari (ed altri non necessari)

Interfacce di rete

- Un PC puo' avere piu' di una interfaccia di rete:
  - interfacce wired
  - interfacce wireless
  - modem
- Ciascuna interfaccia, per poter comunicare via TCP/IP, deve essere configurata con i parametri visti prima

Parte II

Servizi disponibili

server di rete

- Per server di rete si intende generalmente un calcolatore che fornisce un qualche servizio via rete
- Il "servizio" (o server) e' un programma che resta in ascolto sulla rete, ed aspetta che un client gli chieda qualcosa
- La comunicazione tra il client ed il server e' regolata da un protocollo che dipende dal servizio stesso

servizi

- Chiunque puo' scrivere una applicazione di tipo client-server, inventandosi lo scopo ed il protocollo
- Per il funzionamento della rete esiste una notevole quantita' di servizi che sono definiti in modo standard, in documenti noti come RFC (Request For Comment) e numerati

servizi su una macchina linux

- Come per gli applicativi, anche per i servizi esistono in rete numerose implementazioni scaricabili gratuitamente ed installabili per poter utilizzare una macchina linux come server di rete
- Spesso tali programmi sono piu' stabili ed efficienti di corrispondenti programmi a pagamento che si trovano su sistemi proprietari

importante nota sui server

Spesso i server in rete interagiscono tra loro in modo potenzialmente distruttivo.

In virtu' di cio':

non va **MAI** installato ed attivato un servizio di rete senza aver preso accordi espliciti con l'amministratore della rete a cui il PC si connette.

DNS

- Il DNS server e' un server che risponde a richieste relative alla associazione indirizzo IP-nome
- Il programma piu' diffuso (non solo in ambiente linux) si chiama bind
- E' relativamente semplice ed affidabile utilizzare una macchina linux come DNS server

Web

- Il web server e' un programma che, a richiesta, fornisce dati via protocollo http
- E' l'oggetto che viene sempre contattato dai browser quando si digita una URL del tipo html://www....
- Uno dei software piu' diffusi, scaricabile gratuitamente, che implementano il web server si chiama apache
- Molti web server al mondo sono macchine linux

Mail

- Il mail server e' un programma che serve ad inviare e recapitare posta elettronica
- Il piu' diffuso mail server gratuito si chiama sendmail
- Una macchina linux con sendmail e' un mail server affidabile (ma non semplice da configurare)

Mailbox

- Con questo termine ho inteso indicare il server che gestisce l'archiviazione e fornisce accesso alle mail degli utenti
- Esistono diversi programmi che fanno cio' con diversi protocolli (pop, pop3, imap)
- Per ognuno di questi, esiste una versione gratuita che gira su linux, con ottime prestazioni ed affidabilita'

Time

- Un time server e' un programma che serve a sincronizzare un calcolatore via rete
- L'utilizzo di applicazioni di rete rende spesso la sincronia una necessita'
- Esistono diversi protocolli che fanno cio', ed implementazioni gratuite per molti di essi installabili su linux

DHCP

- Gia' visto in precedenza.
- Esiste una implementazione (dhcpd) gratuita per linux.

Authentication server

- La user authentication puo' essere operata localmente o tramite un server
- Esistono diversi meccanismi e protocolli (NIS, Kerberos, LDAP, ...)
- Per ciascuno di questi esistono implementazioni gratuite per linux, affidabili e spesso all'avanguardia nello sviluppo

Disk server

- Esiste la possibilita' di accedere a dati che sono fisicamente collocati su macchine diverse dalla propria, ma che vengono visti come se fossero locali
- Ci sono diversi protocolli con implementazioni disponibili gratuitamente su linux che permettono l'accesso remoto ai dati (NFS, AFS, samba, ...)

Login server

- Esiste la possibilita' di rendere disponibile la CPU e le applicazioni di una macchina per utenti che vi accedono via rete, tramite una login remota
- Ci sono diversi protocolli (telnet, rsh, ssh) con implementazioni gratuite per linux

File server

- Un file server e' un servizio che permette di prelevare o depositare files su un server
- Esistono diversi protocolli che implementano questo servizio (ftp, sftp, bbftp, ...)
- Esistono implementazioni gratuite per linux

X server

- Un X server e' un servizio che permette ad un client remoto di aprire finestre grafiche sul monitor direttamente connesso alla macchina server
- Una implementazione di X server e' disponibile gratuitamente per linux (gia' visto)

Altri server...

- News server, chat server, font server, whois server, talk server, ...
- Il fatto che una macchina linux sia una workstation o un server di rete dipende non dal kernel installato, ma dagli applicativi server installati, configurati e attivati sulla macchina

Linux come server

- Nel fornire un servizio si deve considerare l'affidabilita' di tutte le sue componenti
- Il problema non e' linux, che e' idoneo a fornire servizi di rete, ma:
  - l'affidabilita' dell'hardware
  - la manutenzione del software
  - il monitoraggio degli accessi
  - l'affidabilita' della connessione in rete

Parte III

Linux in rete

Login remota: telnet

- E' possibile eseguire una login remota tramite il server telnetd
- Il client esegue l'applicazione client telnet:

  # telnet <hostname>

  specificando il nome della macchina a cui si desidera connettersi
- Verra' richiesto username e password
- Dopo l'autenticazione si dispone di una finestra di terminale per eseguire comandi sulla macchina remota
- telnet e' un protocollo insicuro

Login remota: ssh

- sshd (secure shell) e' un server che permette di accettare una login remota in modalita' sicura

  # ssh <username>@<hostname>

- Tutta la comunicazione tra il client ed il server avviene in modalita' criptata
- La connessione si presenta in modo del tutto simile a telnet

Esecusione remota di comandi

- Esiste un servizio (rshd) che permette al client rsh l'esecuzione remota di comandi:

  # rsh <host> <cmd>

  Il server accetta la connessione dal client, ed esegue il comando specificato
- Si deve opzionalmente specificare username e password
- La connessione via rsh e' insicura

Esecusione remota di comandi (cont.)

- Il server sshd ed il suo client ssh permettono anche l'esecuzione remota di comandi:

  # ssh <user>@<host> <cmd>

  in modo del tutto simile ad rsh
- Tuttavia la comunicazione tra server e client e' sicura (criptata)

Copia di files (ftp)

- Il server ftpd accetta connessioni (tramite il client ftp) che permettono lo scambio di files tra il client ed il server:

  # ftp <host>

- La connessione richiede una autenticazione
- Dopo l'autenticazione esistono comandi (put, get) per prendere o mettere file sul server
- Esistono comandi (ls, cd) che permettono di navigare nel file system remoto
- La comunicazione via ftp non e' sicura

Copia di files (sftp)

- Il server sftpd accetta connessioni (tramite il client sftp) che permettono lo scambio di files tra il client ed il server:

  # sftp <user>@<host>

  in modo del tutto analogo ad ftp
- La comunicazione via sftp e' pero' sicura

Copia di files (scp)

- E' possibile trasferire files utilizzando un client apposito di sshd: scp
- La sintassi del comando e'

  # scp <file> <host>:<file>

- Viene richiesta una autenticazione, e la comunicazione e' sicura
- Non e' pero' possibile navigare il file system remoto

Copia di files (wget)

- Esiste un client del server httpd (wget) che permette di scaricare files da un sito web:

  # wget <URL>

- Ci sono opzioni che permettono di scaricare recursivamente tutti i files puntati dalla prima URL in modo da generare localmente una copia del sito

Condivisione di files

- Esiste un protocollo (NFS) che permette di condividere files tra PC remoti
- Il server esegue il programma mountd, a cui si puo' dire di "esportare" un sottoalbero di directory (anche un file system completo)
- Il client esegue un comando (mount) per "montare" il file system remoto su un mount point locale:

```
# mount <host>:<dir> <mountpoint>
```

Condivisione di files (cont.)

- In questo modo tutto il sottoalbero sara' accessibile attraverso il mount point come se fosse un altro HD locale
- Generalmente il comando *mount* puo' essere dato solo da root
- Non viene richiesta autenticazione per l'accesso ai files, ma il server puo' essere configurato per esportare files solo a determinati host

Condivisione di file con Windows

- E' possibile accedere ad un "export" di Windows, tramite il programma client smbclient:

  # smbclient \\\\<host>\\<export>

  La presenza dei "doppi \" serve per operare l'escape sul carattere "\"
- Si apre una specie di shell che permette di navigare nel file system remoto e prendere o depositare files (in modo simile a ftp)

Condivisione di files con Windows (cont.)

- Esiste un server (samba) che permette ad una macchina linux di esportare un file system verso macchine windows
- La configurazione del server samba non e' banale
- Il client windows puo' accedere al file system esportato come se il server fosse un'altra macchina windows

X in remoto

- Come gia' visto, l'X server e' capace di accettare finestre grafiche da parte di client remoti
- Sulla macchina client, ogni applicazione X guarda il valore della variabile di environment DISPLAY per sapere dove inviare le immagini
- Il valore della variabile DISPLAY deve essere della forma:

  <host>:<Xserver>.<screen>

  Dove Xserver e screen usualmente valgono 0

X in remoto (cont.)

- L'utilizzo tipico e' il seguente:
  - Ci si collega in remoto da PC1 a PC2 (ad esempio tramite ssh)
  - Sulla macchina PC2 si definisce la variabile DISPLAY per puntare all'X server di PC1 (quella con attaccato il monitor che abbiamo davanti agli occhi):

    ```
    # export DISPLAY=PC1:0.0
    ```
  - Si esegue su PC2 una applicazione X
  - L'immagine apparira' sul monitor di PC1

X in remoto (cont.)

- E' possibile configurare l'X server per rifiutare connessioni da parte di client non esplicitamente specificati
- Questa configurazione e' consigliata per motivi di sicurezza
- Si opera questa configurazione tramite il comando *xhost*

X in remoto (cont.)

xhost + (si attiva la protezione)

xhost + <client> (si permette al client di aprire finestre grafiche sul server)

xhost - (si disattiva la protezione: tutti possono aprire finestre grafiche - e visualizzare i caratteri digitati sulla tastiera del server)

X in remoto (cont.)

- Esistono X server che girano in ambiente Windows (XWin32, Exceed)
- Questi programmi permettono di utilizzare applicazioni grafiche X quando siamo connessi in remoto su una macchina unix anche se il desktop e' una macchina windows