

Corso Di Linux

Liceo Fermi, Bologna - Marcello Galli, novembre 2009

La Rete, nozioni di base.

Il protocollo (regole di comunicazione), usato dalla rete internet si chiama TCP/IP. Il TCP/IP descrive tutti i dettagli su come i computer si parlano attraverso la rete. Qui si descriveranno solo i punti essenziali del TCP/IP, che servono per usare Linux in rete.

La rete internet, come la conosciamo oggi, deriva dalle reti americane degli anni 70, quando il ministero della difesa americano, in piena guerra fredda, inizio' a finanziare studi per una rete di computers che fosse adatta a resistere ad attacchi nucleari del nemico.

Al progetto lavorarono molto all'universita' del Berkeley ed al MIT, siccome nelle universita', in quel periodo, era diffuso Unix, presto il software per collegare i computers in rete fu incluso nel sistema Unix; Unix e la rete internet crebbero insieme.

Per resistere agli attacchi nucleari internet non ha un centro; altrimenti il nemico, attaccando il centro, potrebbe distruggere tutta la rete. I computers sono collegati gli uni agli altri in modo libero, attraverso percorsi multipli; i dati che viaggiano fra i computers sono divisi in pacchetti, e pacchetti diversi possono fare anche strade diverse per arrivare a destinazione; in questo modo i computers possono continuare a parlarsi anche se il nemico distrugge qualche collegamento. Questo modo di trasmettere i pacchetti si chiama "packet switching".

Il Routing

I computer dedicati ai collegamenti si chiamano *routers*, i routers hanno molti collegamenti: ad altri routers oppure a computer normali. Ogni collegamento ha un suo spinotto ed un suo cavo. Le diverse uscite di un router si chiamano *interfacce di rete*.

Sul router c'e' un programma che decide cosa fare dei pacchetti che arrivano dalle diverse interfacce. La decisione e' presa in base ad una tabella, che si chiama "tabella di routing"(routing table). Nella tabella c'e' scritto quale computer o rete di computer e' collegata alle diverse uscite. Nel pacchetto di dati che arriva c'e' scritto l'indirizzo ed il router decide a quale uscita girare il pacchetto in base all'indirizzo. Se non trova l'uscita adatta lo manda ad un'uscita di default (che si chiama default route), oppure, a seconda di come e' configurato, lo butta via ed il pacchetto e' perso.

Un router puo' essere pensato come un incrocio stradale, con tanti cartelli, che danno indicazioni per raggiungere diverse localita'. I cartelli sono un po' come una tabella di routing, che si consulta per sapere dove andare, e come un router collega piu' reti, cosi' l'incrocio collega piu' strade.

Ogni computer e' un po' un router, pero' ha una sola uscita. La sua tabella di routing e' molto semplice.

Hub e switch

Spesso i computers non sono collegati direttamente ad un routers, ma ad un apparato di collegamento, che si chiama switch (i vecchi modelli si chiamavano hub), l'apparato di collegamento e' poi connesso al router. Questo apparato di collegamento manda tutti i pacchetti che gli arrivano al router. Oppure, se due computer collegati vogliono parlare fra loro, manda i pacchetti di uno all'altro e viceversa.

Indirizzo dei computers

L'indirizzo del computer e' un numero, si chiama numero IP; in genere e' scritto raggruppando le cifre in 4 gruppi, separate da un punto, ad esempio: 192.168.2.32. E' scritto cosi' perche' ogni gruppo di cifre rappresenta un byte, ed il numero IP e' grande 4 bytes: 32 bits. I primi di questi bits rappresentano il numero della rete cui e' attaccato il computer, gli ultimi il numero del computer nella rete. Ci sono reti con molti computer e reti con pochi computer, per cui si puo' scegliere quanti bit usare per la rete e quanti per i computer della rete. C'e' quindi un altro numero, associato all'indirizzo, che si chiama maschera di rete (network mask), che dice appunto quanti sono i bit usati per la rete e quanti per i computers. Nel nostro esempio, se scriviamo la network mask con: 255.255.255.0 abbiamo che la rete ha il numero: 192.168.2 il computer e' il numero 32.

I routers decidono dove inviare i pacchetti in base alla parte di indirizzo che riguarda la rete, i routers sono usati quindi per collegare reti diverse, anche se potete usarli anche per collegare computers.

Quando i computer sono sulla stessa rete non usano per inviarsi pacchetti il numero IP, ma un altro numero fa da indirizzo; quello della scheda di rete. Il numero della scheda di rete e' utilizzato per gestire la trasmissione dei dati dalla scheda di rete ai cavi e viceversa. Il protocollo di comunicazione e' diverso, e si chiama ethernet; il protocollo che si usa per le reti senza fili e' simile ad ethernet, ed anche li' la scheda di rete (scheda wireless) ha un numero che la identifica.

L'uso del numero della scheda di rete e' dovuto al fatto che le schede di rete non sanno nulla di numeri IP; i computer della stessa rete sono collegati tutti insieme e sugli stessi fili passano i pacchetti di tutti; per capire quali sono i suoi pacchetti la scheda di rete guarda se hanno come indirizzo il suo numero di scheda. Quando vede pacchetti suoi li prende, e li passa al software di rete. Oppure prende i pacchetti destinati contemporaneamente a tutti i computers, che si chiamano *broadcast*.

Gli hub e gli switch, usati per collegare computers della stessa rete, utilizzano, per sapere a che uscita sono collegati i computers, il numero della scheda di rete, non i numeri IP.

In definitiva i computers hanno 2 numeri che fanno da indirizzo, quello della scheda di rete, utilizzato per trasmissioni sulla stessa rete (per mettere i pacchetti sul filo), e quello IP, che serve ai router per mandare i pacchetti a reti diverse.

Porte

Si chiamano porte dei canali di comunicazione che servono ai programmi per parlare al software di rete e lavorare in rete. Le porte sono numerate, e, quando arrivano i pacchetti, il software di rete utilizza il numero della porta per sapere a che programma dare i dati che arrivano.

Quando un programma vuole comunicare con un programma di un altro computer *apre* una porta, e, tramite questo canale, manda i suoi dati al software di rete, che li impacchetta e li invia a destinazione.

Un programma puo' anche essere un programma di tipo server, che offre servizi, ed allora *apre* una porta e si mette in ascolto da quella porta; quando da un altro computer arriva un pacchetto per la sua porta il software di rete lo spacchetta e gli passa i dati tramite la porta.

Un pacchetto che viaggia in rete ha quindi associati 4 numeri che fanno da indirizzi:

- il numero IP del computer di origine
- il numero della porta che il programma sul computer di origine ha utilizzato.
- il numero IP del computer di destinazione
- il numero della porta del programma sul computer di destinazione.

In piu' c'e' il numero della scheda ethernet, che pero' viene usato solo per regolare la trasmissione sul cavo.

Abbiamo detto che le porte sono numerate, molti numeri hanno un significato prestabilito per convenzione, ad esempio il server web sta in ascolto dalla la porta 80, per mandare posta si usa la porta 25, etc. etc.

Le porte sono di 2 tipi: TCP ed UDP, infatti ci sono 2 modi diversi di collegamento:

- TCP (detto anche connection oriented)
- UDP (detto anche connectionless)

Nel collegamento TCP si tiene conto di tutti i pacchetti e se vengono persi nel percorso si ritrasmettono, nell'UDP si manda un messaggio e basta, non si sta ad aspettare conferma di arrivo dei pacchetti. UDP si usa per messaggi brevi, dove non importa se qualcosa si perde o se l'altro computer non risponde bene.

Nomi e numeri di computer

Il TCP/IP usa numeri per identificare i computers nella rete, ma agli umani piace usare dei nomi, per cui i computers in rete, oltre che un numero, hanno anche un nome. I nomi dei computers sono fatti con campi separati da punti, come ad esempio: `www.helldragon.eu`; i campi riflettono una struttura gerarchica ed i vari livelli della gerarchia sono chiamati "domini" e sono gestiti da organizzazioni diverse.

I nomi dei computer sono infatti conservati nel DNS (Domain Name System), un database distribuito, nel senso che ogni organizzazione gestisce la sua parte, e mantiene un computer con un programma per DNS che, a richiesta, fornisce i nomi ed i numeri dei computer dell'organizzazione. Se il dominio ha dei sotto-domini, il programma fornisce, a chi lo chiede, l'indirizzo del computer che ha il DNS del sotto-dominio.

Facciamo un esempio; prendiamo il nome `www.helldragon.eu`; `.eu` indica il dominio dell'Unione Europea, che ha incaricato la società Eurid di gestire un DNS con i nomi che finiscono in `.eu`. Eurid ha dei computer con il programma per il DNS ed ha scritto nel suo DNS il nome `helldragon` assieme al numero IP del computer che gestisce `helldragon`. Questo è un computer del mio internet provider, dove io metto i nomi delle mie macchine, che finiscono tutte con: `helldragon.eu`.

Quando un browser web vuole collegarsi a `www.helldragon.eu`, prima deve scoprire il numero IP di `www.helldragon.eu`. Per fare questo si collega al computer che gestisce il dominio `.eu` e gli va a chiedere il numero IP di `www.helldragon.eu`. Ma quel computer gli risponde che lui gestisce `.eu`, non `helldragon.eu`, il numero non lo sa; però gli dà il numero IP di chi gestisce il sotto-dominio `helldragon.eu`. Il browser a questo punto va a chiedere al computer gestore di `helldragon.eu`, e finalmente gli arriva in risposta il numero IP di `www.helldragon.eu`. Solo a questo punto il browser può collegarsi al mio sito web, utilizzando il suo numero IP.

La ricerca di un nome procede quindi per via gerarchica, a partire dai domini principali (detti root domain). In realtà non è sempre così, i computer hanno programmi che ricordano i nomi ed i numeri IP già usati, ed inoltre si può chiedere ad un DNS di fare tutta la ricerca per voi e non dovete tutte le volte iniziarla dal dominio principale.

Resta il fatto che per utilizzare nomi di computer e non dover usare sempre i numeri, dovete dire al vostro PC a chi chiedere i numeri IP, cioè dargli l'indirizzo IP di un computer con un programma per DNS.

IP pubblici, privati e prestati

Alcuni numeri IP non sono usati in internet, ma ognuno può usarli per farsi una rete privata con computers che non sono collegati ad internet. I routers di internet non dovrebbero mandare pacchetti a questi indirizzi. Questi indirizzi si chiamano IP privati e sono quelli che iniziano con 10, oppure con 192.168 ed alcuni degli indirizzi che iniziano con 172.16. Gli altri numeri sono detti IP pubblici e sono numeri di computer connessi ad internet.

Il numero IP pubblico di un computer è unico, ogni computer deve avere il suo. Però, con soli 32 bits per gli indirizzi, non ci sono abbastanza numeri per tutti i computer del mondo. Dicono che fra 2 anni i numeri saranno finiti e non si potranno più collegare nuovi computers; c'è in progetto di fare un nuovo TCP/IP, con indirizzi lunghi e numeri per tutti (IP versione 6), ma siamo ancora indietro, per cui si ricorre ad alcuni trucchi.

Uno è quello dei numeri IP in prestito. Quando voi vi collegate in internet vi connettete al vostro provider, che a sua volta è collegato ad internet; quando vi connettete il provider assegna alla vostra

macchina un numero dei suoi, ma ve lo presta solo, quando vi scollegate lo presta ad un altro. Quando vi collegate un'altra volta vi presta ancora un numero, ma non e' detto che sia sempre lo stesso, il vostro numero cambia. In questo caso si dice che si ha un numero IP dinamico.

Si puo' anche fare un contratto che vi garantisce un numero IP tutto vostro, sempre quello, ed in questo caso si dice che si ha un numero IP statico. Gli IP statici costano di piu'.

Un altro trucco e' utilizzare lo stesso numero IP per molti computers: poniamo che abbiate una vostra rete privata, ai cui computer avete dato numeri che iniziano con 192.168, come 192.168.7.10 . Uno di questi computer, ad esempio il 192.168.7.254, e' un router, e' collegato ad internet, ed ha 2 interfacce di rete, una, dalla parte della rete interna, con numero 192.168.7.254, ed una esterna, con un IP pubblico. Questo computer, tramite la sua interfaccia pubblica, puo' parlare con i computer di internet, ma gli altri computer, nella rete interna, privata, non possono; non hanno numeri pubblici, riconosciuti in internet, ma solo numeri privati.

Il trucco e' che il router fa i collegamenti ad internet per conto dei computer interni, usando il suo IP pubblico. Questo si chiama NAT: "network address translation". I computer interni hanno nella loro routing table istruzione di mandare le richieste di collegamento internet al router, il router fa lui i collegamenti internet, inoltra i pacchetti per conto loro e manda indietro i pacchetti di risposta che riceve.

In questo modo i computer interni possono fare collegamenti verso internet, ma non e' possibile il contrario, dall'esterno non e' possibile fare collegamenti verso di loro, non hanno IP pubblico ed il mondo vede solo il router. Anche i collegamenti dei computer interni verso l'esterno sono visti tutti come provenienti dal router.

Alcuni router permettono di girare alcune porte (port forwarding). Cioe' quando da internet arriva un pacchetto per una certa porta lo mandano ad uno dei computer interni predefinito. In questo modo potete rendere i computer interni visibili da internet, ma solo da certe porte. Questo serve per certi programmi peer-to-peer o per certi giochi in rete.

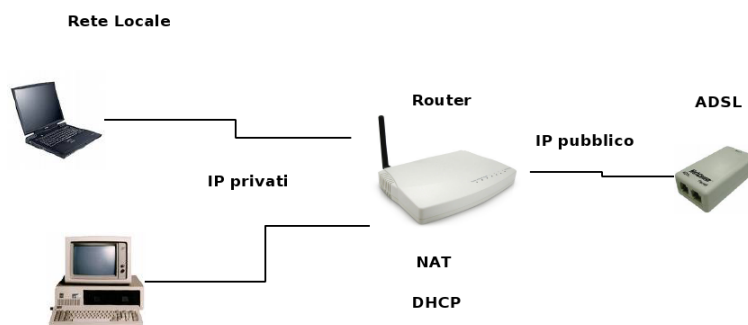


Figure 1: La tipica rete di casa

Configurazione di un PC linux per collegarsi in rete

In definitiva per far lavorare il vostro PC in rete dovete:

- dargli un numero IP;
- mettere almeno l'indirizzo di un router di default nella sua routing table;
- dargli il numero IP di un computer col DNS;
- ovviamente dovete avere la scheda di rete coi cavi attaccati ed il driver giusto caricato nel kernel ;

Puo' sembrare un lavoro brigosio, ma ormai la maggior parte delle distribuzioni hanno reso tutto automatico. C'e' un programma, che si chiama DHCP (DHCP sta per "Dynamic Host Configuration Protocol") che assegna numeri IP, per cui se, nella rete cui vi connettete, c'e' un qualche computer con un servizio DHCP il numero IP ve lo da lui.

Se configurati per farlo, i PC, all'accensione, mandano sulla rete messaggi di richiesta ad un programma DHCP, che gli risponde assegnandogli un numero IP e dandogli tutte le informazioni necessarie per configurare il software di rete; come l'indirizzo di un server DNS, informazioni di routing etc. Il DHCP e' ora molto diffuso. Solo se il DHCP non c'e' sulla rete o non vi risponde, dovete configurare tutto voi.

E' ormai molto diffusa la connessione ADSL per i collegamenti in rete. ADSL e' un modo di comprimere al massimo i segnali elettrici che codificano i pacchetti, in modo da poterli fare andare veloci sui normali fili del telefono. E' un sistema di compressione veramente complicato, ma vi consente di andare a velocita' di alcuni megabit/secondo su fili su cui, solo 10 anni fa, si andava al massimo a velocita' attorno ai 20 kilobit/secondo.

In genere in casa avete attaccato al cavo del telefono uno splitter, un piccolo apparecchio che separa i segnali del telefono da quelli per il computer. Dallo splitter escono 2 fili, uno va ai vostri telefoni, uno ad un router. I vostri computer sono poi attaccati al router. Il router ha 2 interfacce di rete, una verso i vostri computers, l'altra verso l'ADSL ed il vostro provider, e si collega al router del vostro provider.

Questi router costano poco, si fanno prestare automaticamente un numero IP dal vostro provider quando vi collegate, hanno dentro un programma per DNS, un programm per DHCP, e fanno il trucco del NAT per fare uscire su internet i computer della vostra rete interna. Si configurano con una facile interfaccia web. Essenzialmente dovete dargli la password che vi ha dato il provider. Il resto e' tutto automatico. Se non avete esigenze particolari non dovete fare assolutamente nulla per collegarvi in rete, il vostro router ADSL fa tutto da solo.

Ma resta il fatto che oggi ognuno finisce per avere in casa un router e forse sarebbe meglio se avesse un'idea di cosa questo router fa per poterlo usare al meglio e non essere nei guai se qualcosa va storto. Ad esempio a volte certi programmi richiedono che si possa accedere ad un computer della vostra rete interna dall'esterno (certi giochi o programmi per il peer-to-peer); si puo' istruire il router perche' mandi i pacchetti che gli arrivano dall'esterno su certe porte a computer della vostra rete interna. Questo si chiama "port forwarding".

Poniamo ad esempio che abbiate messo delle vostre pagine web ed un programma server (per distribuirle a chi le chiede) su un PC di numero: 192.168.10.5; il vostro server web ascolta connessioni che arrivano dalla porta 80; ma e' visto solo dalla rete interna. Perche' chi si collega dall'esterno al vostre router possa vedere le vostre pagine web dovete dire al router: "le richieste di collegamento che arrivano dall'esterno sulla tua porta 80 mandali alla porta 80 del computer numero 192.168.10.5". Non e' una cosa difficile, le interfacce grafiche di questi ruter sono semplici; ma per farlo bisogna capire cosa si sta facendo.

Utilizzo di Linux in rete

Configurazione del software di rete

Vediamo come si configura Linux per l'uso della rete nel caso non ci sia in giro un programma DHCP che ci aiuta. Qui facciamo riferimento ad una distribuzione Linux Knoppix 5.1.1, ma le procedure sono simili per le diverse distribuzioni.

Si puo' procedere nei seguenti modi:

- 1- Tramite interfaccia a comandi:** si apre una finestra terminale, e si diventa root in quella shell; configurare la rete e' un'operazione privilegiata che e' impedita agli utenti normali, dovete essere l'utente di servizio per farla.

In Knoppix 5.1.1 potete farlo cliccando sul menu con la K, poi sul sotto-menu "knoppix" scegliete l'opzione: "root shell" A questo punto fate tutto dando comandi in questa finestra terminale (che si chiama root shell).

- Per vedere come e' messa l'interfaccia di rete si da il comando:

ifconfig

Se il nome dell'interfaccia e' eth0 ed il numero che si vuole dare alla macchina e' 192.168.100.101, si configura l'interfaccia con:

ifconfig eth0 192.168.100.101 netmask 255.255.255.0 up

per controllare che tutto sia a posto date ancora il comando:

ifconfig

- Si controllano le routing tables, con il comando:

route

Si nota come si vede semplicemente la rete: 192.168.100.0, direttamente collegata all'interfaccia di rete eth0.

Se una macchina della LAN fa da router, collegata anche all'esterno, per uscire dalla LAN si dovrebbe inserire una default route verso questa macchina; se il router ha l'IP 192.168.100.1 daremo il comando:

route add default gateway 192.168.100.1

2- Utilizzando un'interfaccia grafica, (in Knoppix 5.1.1 e' il menu Knoppix, quello col pinguino, alla voce network -> opzione network card.) Le operazioni da fare sono le stesse, ma mettete i dati in un modulo grafico invece che scriverli sul terminale.

Ci sono una serie di comandi che servono per controllare la rete, i piu' importanti sono:

- */sbin/ifconfig* : vi fa vedere l'interfaccia di rete o la configura
- */sbin/route*: vi fa vedere o modificare le tabelle di routing
- *netstat* : vi fa vedere come e' messa la rete; ha molti parametri;
 - *netstat -nltup* : vi fa vedere le porte aperte, da cui qualche programma accetta connessioni esterne. Se lo date quando siete root vedete anche che programma usa la porta (opzione p) altrimenti no, un utente normale non e' abilitato.
- */sbin/arp* : vi fa vedere i numeri delle schede ethernet dei computer della vostra rete, ma non li vedete tutti, il vostro computer li conosce quando qualcuno si collega a lui, poi li dimentica in fretta.
- *ping* : manda un messaggio alla scheda di rete di un computer, per vedere se funziona e risponde.
- */usr/sbin/traceroute* : vi fa vedere che percorso fanno i pacchetti fra i routers per andare ad una macchina lontana.
- *host* : comando che interroga il DNS, se gli date un nome di computer risponde col numero IP, e viceversa.

Diagnostica

Capita a volte che qualcosa in rete non vada, per capire quale e' il problema e rimediare, occorre procedere in modo sistematico, consiglio le seguenti azioni, nell'ordine:

1. controllare i cavi, ed eventuali lucine su switch e schede di rete, le lucine lampeggiano quando passano i pacchetti; spesso si e' solo staccato od allentato un cavo
2. la scheda di rete e' configurata bene ? Controllate usando il comando *ifconfig*, guardate se e' in stato "up" e se ha un numero IP.

3. Il software di rete e' a posto ? Usate il comando ping, prima fate un ping su voi stessi, con: *ping localhost* poi provate a collegarvi a voi stessi, con un comando tipo telnet od ssh (che vedremo dopo). Se riuscite a collegarvi a voi stessi il software di rete e' a posto.
4. Provate a veder se raggiungete il router, fate ping con l'indirizzo IP del router. Se non lo raggiungete c'e' qualcosa sul percorso da voi al router che non funziona.
5. Usate il comando *traceroute* per vedere fin dove arrivano i vostri pacchetti. arrivano al router, dove si fermano ?
6. E' il DNS che non va? Usare il comando *host* per provare a chiedere un nome di computer. Spesso non funziona il dns e la gente crede sia un problema di rete, invece sono solo i nomi che non vengono tradotti in numeri IP.
7. In caso non capiate proprio cosa sta succedendo potete provare ad usare uno sniffer per vedere i pacchetti che passano per il cavo cui siete collegati, ma dovete conoscere un po' il protocollo di rete il TCP/IP per capirci qualcosa.

Uno sniffer e' un programma che mette la scheda in uno stato che si chiama: "modo promiscuo", in cui la scheda prende dalla rete tutto, non solo i suoi pacchetti. Lo sniffer vi fa quindi vedere i pacchetti, o potete metterli in un file per esaminarli con calma. Lo sniffer e' famoso come programma per spiare le password, ma in realta' e' uno strumento diagnostico di base. Uno sniffer grafico e' wireshark, oppure potete usare il comando *tcpdump* da una finestra terminale. Il comando *tcpdump* ha molti parametri complicati.

Alcuni applicativi da usare in rete

- *ssh* : una cosa che si fa spesso in rete e' collegarsi ad un'altra macchina con una finestra terminale (una shell), e lavorare sull'altra macchina usando il video e la tastiera della vostra. Il comando per fare questo e' *ssh* (sta per secure shell): aprite una finestra terminale (una shell) sul vostro computer, poi date il comando: *ssh nomealtrocomputer* venite collegati all'altro computer che vi chiede la password (quelle dell'altro computer, non quella del computer da cui state lavorando). A questo punto la finestra terminale e' come trasferita sull'altro computer.

Una volta al posto di *ssh* si usava *telnet*, che fa la stessa cosa, ma *ssh* in piu' cripta tutti i dati che passano fra i 2 computers. Con *telnet* era facile spiare le password, per cui ora si usa *ssh* che e' piu' sicuro.

- server *ssh*: la macchina a cui vi collegate con *ssh* deve avere attivo un "server *ssh*", un programma che sta in ascolto dalla porta 22 e regola le richieste di connessione in arrivo. In genere le distribuzioni hanno questo servizio gia' attivato. Se non lo e', come ad esempio su *knoppix*, dovete farlo partire. Anche qui potete procedere in 2 modi:

- da una shell di root date il comando: */etc/init.d/ssh start*
- oppure usate l'interfaccia grafica, in *knoppix* seguite i menu: *knoppix*: -> server -> start *ssh*

- *ftp* : o la sua variante che cripta i dati: *sftp*. Questo comando serve a trasferire dati fra 2 computers. Quando fate un sito web e poi lo "pubblicate" in realta' state trasferendo le vostre pagine sul server con *ftp*. Anche qui fate: *ftp nomealtramacchina* e poi potete dare una serie di comandi ad *ftp*:

- *help* : da aiuto
- *ls* : mostra i files sull'host remoto
- *cd* direttorio : si cambia direttorio sull'host remoto
- *pwd* : mostra direttorio corrente sull'host remoto

- get file : prende un file
 - put file : mette un file sull'host remoto
 - mget * : prende tutti i files del direttorio corrente
 - mput * : mette tutti i files
 - !ls : mostra files sull'host locale
 - !pwd : mostra direttorio corrente sull'host locale
 - ! cd .. : ci si sposta in su di un livello sull'host locale
 - type binary : i dati sono trasmessi senza modifiche (dati binari)
 - **type ascii (trasmette testi e converte carriage return/linefeed in linefeed)**
(serve solo se si trasferisce da sistemi non unix)
 - bye : si esce dal programma ftp.
- http server: oggi la maggior parte del traffico di rete utilizza il protocollo httpd, che e' quello che stabilisce come vengono trasmesse le pagine web. Ogni distribuzione Linux ha un server web. Per cui potete fare le vostre pagine, e far partire il server. Il server si mette in ascolto sulla porta 80, che e' la porta cui i client, come mozilla, firefox od internet explorer, fanno le connessioni per chiedere le pagine web. Chi riesce a raggiungere via rete la vostra macchina potra' vedere le vostre pagine.

Usare applicativi grafici in rete

Il sistema grafico di Unix: X11 permette di lavorare alla consolle di una macchina, collegati su un'altra e di aprire applicazioni grafiche su un'altra macchina ancora.

Per fare questo su usa una finestra terminale, collegata, con ssh o telnet, ad un computer remoto e si definisce la variabile di shell DISPLAY, che dice su che schermo di che macchina devono essere mandate le applicazioni grafiche. A questo punto se date comandi che fanno partire applicazioni grafiche queste verranno mandate al video scelto.

Per fare questo occorre che l'X11 abbia attivo un servizio di rete in ascolto sulla porta 6000. In molte distribuzioni questa possibilita' e' disabilitata, per questioni di sicurezza. In knoppix 5.1.1 dovrebbe essere abilitata.

Vediamo con un esempio come si procede:

- a) aprite una finestra terminale e vi collegate ad una macchina remota. Oppure dalla vostra macchina potete

Unexpected indentation.

mandare i grafici ad una macchina remota.

- b) definite la variabile DISPLAY, con un comando tipo:

```
export DISPLAY=192.168.100.101:0.0
```

questo manda il video aulla macchina di IP:192.168.100.101, sullo schermo numero 0 (ma in genere lo schermo e' uno solo)

Per ri-dirigere il display sulla macchina locale: *export DISPLAY=:0*

- c) sulla macchina su cui state mandando le immagini dovete togliere la protezione dello schermo, non e' che uno puo' usare uno schermo se il proprietario non vuole.

Ci sono modi piu' sicuri di procedere, ma il sistema piu' semplice e' usare il comando xhost. Da una finestra terminale della macchina su cui volete mandare la grafica fate:

- xhost + : tutti accedono al video

- xhost + 192.168.100.101 : questa macchina accede
- xhost - 192.168.100.101 : questa macchina non accede piu'

d) adesso far partire applicazioni grafiche e le immagini appariranno sullo schermo che avete deciso:

Per esempio:

- xclock & : fa apparire un orologio
- xterm & : fa apparire una finestra terminale

Per utilizzare la grafica in rete ci vuole un collegamento veloce, attorno a qualche Mbit/secondo. In genere si fa su una rete locale ethernet, ove la velocita' e' almeno 10 Mbit/sec.

Condivisione dischi

Ci sono diversi modi per condividere parti di disco e vederle su piu' macchine come fossero dischi locali; in genere si usa il protocollo nfs (network file system).

Per condividere cartelle con macchine windows si usa il programma samba.

Molte distribuzioni hanno tool grafici per aiutare gli utenti nel configurare le condivisioni. Altrimenti bisogna andare a cambiare alcuni files di configurazione nella cartella /etc e poi far partire i programmi che rendono disponibili i files in rete. E' un argomento un po' piu' complicato dei precedenti.

© Marcello Galli, Novembre 2009. Sito di riferimento: <http://www.helldragon.eu>