

Corso Base su Linux

Basato su Fedora 7
Lezione 4



Configurare la rete

Esistono diversi metodi per configurare il servizio di rete:

- editare i singoli file di configurazione del networking (per applicare le modifiche si deve fare ripartire il servizio di rete);
- usare comandi shell come ifconfig e route
- utilizzare strumenti di configurazione con interfaccia a finestra come setup, netconfig, linuxconf, webmin, system-config-network e altri facilmente individuabili su desktop KDE o GNOME.

Dove possibile si consiglia di usare questi ultimi per la maggiore facilità d'uso.

La modifica manuale dei file di configurazione è complicata dal fatto che nelle varie distribuzioni Linux esistono delle differenze, pertanto i file da modificare variano secondo la distribuzione, benché alcuni ovviamente coincidono.

Le schede di rete vengono indicate con:

<code>eth0 – eth0:1 – eth0:22</code>	La prima scheda di rete, eth0:x sono IP Virtuali
<code>eth1 - eth1:3</code>	seconda scheda di rete e relativi IP Virtuali
<code>ppp0</code>	Point to point



File di configurazione

Quanto riportato di seguito si applica alla distribuzione Fedora 7, in altre distribuzioni il nome dei file e la loro ubicazione può essere differente.

<code>/etc/sysconfig/network</code>	Contiene le principali configurazioni per il Networking: hostname, domainname, default gateway. Esempio con impostazioni base: <code>NETWORKING=yes</code> ; Attiva il networking <code>HOSTNAME=tux</code> ; Nome dell'host <code>GATEWAY=10.0.0.1</code> ; IP del default gateway
<code>/etc/hosts</code>	Contiene il mapping fra indirizzi e hostname ed alias. Segue un esempio. <code>127.0.0.1 localhost.localdomain localhost</code> <code>10.0.0.22 tux.dominio.it tux pinguino</code>
<code>/etc/services</code>	Contiene il mapping tra i numeri di porta e i nomi dei servizi.
<code>/etc/host.conf</code>	Specifica l'ordine secondo il quale il sistema effettuerà la ricerca di informazioni per risolvere gli indirizzi. Usato dalla resolver library in sistemi con libc versione 5. <code>order hosts,bind</code> ; usa prima <code>/etc/hosts</code> e poi DNS per risolvere gli IP.
<code>/etc/nsswitch.conf</code>	Uguale ad <code>host.conf</code> nei sistemi con libc versione 6 (glibc). E' sempre meglio avere entrambi i file correttamente configurati.



File di configurazione

/etc/resolv.conf

File di configurazione del client DNS.
Contiene gli indirizzi dei server DNS e un possibile dominio dell'host e l'ordine di ricerca
nameserver 10.0.0.150 ; IP del DNS server primario
nameserver 192.168.1.10 ; IP del DNS server secondario
domain dominio.it ; Nome del dominio dove si trova l'host
options timeout:6 ; E' il timeout per le query DNS.

/etc/sysconfig/networking/device/ifcfg-eth0

/etc/sysconfig/networking/device/ifcfg-eth0:1

File di configurazione della scheda di rete eth0.

DEVICE=eth0	Nome del dispositivo
BOOTPROTO=none	BOOTP disabilitato
HWADDR=00:11:2f:d1:ca:38	MAC address
ONBOOT=yes	Attivata al boot
DHCP_HOSTNAME=brontolo	nome dell'host
IPADDR=192.168.1.10	indirizzo IP
NETMASK=255.255.255.0	maschera di rete
GATEWAY=192.168.1.1	default gateway



Comandi di shell per configurare la rete

Questi comandi in genere valgono fino al successivo reboot, si usano per verificare una configurazione prima di apportare le modifiche ai file di configurazione.

`ifconfig [interface] [options] | address` Permette di configurare le interfacce di rete.

`Ifconfig` Elenca tutte le interfacce attive e le relative impostazioni

`ifconfig eth0 [up | down]` Attiva o disattiva l'interfaccia eth0

`ifconfig eth2 192.168.0.56 netmask 255.255.255.0`

Configura /dev/eth2 con indirizzo ip 192.168.0.56 (/24)

`route [opzioni] [comando] [parametri]` Permette di manipolare la tabella di routing

`route -n` Visualizza informazioni di routing evitando di risolvere gli ip

`route add -net 192.56.76.0 netmask 255.255.255.0 gw 192.168.0.1`

Aggiunge una route statica per la rete 192.56.76.0/24, usando 192.168.0.1 come gateway

`route add -net 0.0.0.0/0 gw 192.168.0.1`

Imposta 192.168.0.1 come default gateway

A volte è necessario riavviare i servizi di rete per attivare una nuova configurazione, si può fare utilizzando lo script di init : `/etc/init.d/network (start | stop | restart)`

In Fedora si può usare anche il comando: `service network [start | stop | restart]`



Diagnosi della rete

netstat [opzioni]

Interroga `/proc/net/*` e visualizza informazioni sul networking subsystem di Linux permettendo di conoscere lo stato e l'utilizzo dei servizi di rete.

Opzioni utili:

- n Disabilita il reverse lookup
- r Visualizza la tabella di routing
- p Visualizza i programmi che utilizzano la connessione
- s Visualizza statistiche per i singoli protocolli
- a Visualizza tutte le connessioni: attive e in listening

arp [opzioni]

Visualizza e manipola l'ARP cache del sistema.
Estrapola le informazioni da `/proc/net/arp`

Opzioni utili:

- n Disabilita il reverse lookup
- a Visualizza l'arp cache del sistema
- d host Rimuove l'host specificato dalla arp cache



Diagnosi della rete

tcpdump [opzioni] [espressioni]

Tool di packet sniffing, è possibile utilizzare filtri ed effettuare il dump su file. Visualizza le intestazioni dei pacchetti, non il contenuto.

Opzioni utili:

- i eth# Specifica l'interfaccia su cui ascoltare
- c ## Esce dopo aver ricevuto il numero specificato di pacchetti
- r nomefile Utilizza il file specificato come input per i dati da filtrare
- w nomefile Scrive su file il risultato dello sniffing
- n Non risolve i nomi degli host

Le espressioni definiscono i criteri con cui filtrare i pacchetti. Se non vengono definite vengono visualizzati tutti i pacchetti.

type Ha come possibili valori: host - net - port
Es: tcpdump host pippo, tcpdump port 80, tcpdump net 10.0

dir Indica la direzione dei pacchetti: src - dst - src or dst - src and dst
Es: tcpdump src host pippo, tcpdump dst port 80

proto Restringe il dump al protocollo specificato:
ether - fddi - tr - ip - ip6 - arp - rarp - decnet - tcp - udp
Es: tcpdump tcp dst port 80



Altri strumenti di utilità

ping ip

Invia ICMP ECHO REQUEST all'IP specificato.

traceroute [opzioni] ip

Ricostruisce il percorso che effettua un pacchetto verso la destinazione definita, visualizzando tempi medi, minimi e massimi per superare un certo hop.

nslookup [opzioni]

Esegue query interattive a server DNS. Recentemente viene preferito dig.

dig @server domain query-type

Alternativa più dettagliata e completa a nslookup.

lynx [url] e links [url]

Web browser testuali. Links è più evoluto e supporta anche frame

ftp [opzioni] [url]

FTP client. Un'alternativa valida su Linux è ncftp.

wget [opzioni] [url]

Utility polifunzionale per scaricare file via http o ftp. Permette di effettuare il mirror di siti Web (-m)

whois [opzioni]

Esegue un whois lookup

mail email@mail.it

Invia una mail all'indirizzo specificato.



Linux come firewall

La gestione delle funzioni di packet filtering, natting e forwarding dal kernel 2.4 è affidata al netfilter subsystem, gestibile tramite il comando *iptables*.

La gestione delle funzioni di firewalling su Linux ha subito nel corso degli anni cambiamenti progressivi.

Nel kernel 2.x questa funzione è affidata ad un comando con sintassi simile: ipchains.

Nei kernel precedenti il comando utilizzato era ipfadm.

Iptables basa la sua funzionalità su diverse tabelle (tables) a cui sono applicate delle catene (chains) con le regole di filtering definite dall'utente.

La gestione delle tabelle tramite iptables esula dagli obiettivi di questo corso.

Per gestire in modo agevole Linux come firewall si consiglia l'uso di fwbuilder, un frontend grafico che permette di creare le tabelle di firewall in modo visuale, verificarne la correttezza e applicarle al sistema.

Sempre usando yum:

```
$ yum install fwbuilder
```

che dovrebbe installare queste dipendenze se non presenti: fwbuilder, libfwbuilder, fwbuilder-ipt, fwbuilder-ipf o fwbuilder-pf, gcc, gdk_pixbuf, glib, glibc-2.2.4, gtk, gtkmm, libsigc++, libstdc++, libxml2, libxslt, libz, openssl-0.9.6b, ucdsnmp, xshared



Server Web

In Linux il server http standard è **Apache**.

Se già non è presente sul sistema si deve installare: `$ yum install httpd`

I pacchetti necessari per un'installazione tipica verranno selezionati automaticamente.

I file di configurazione si trovano nella directory `/etc/httpd`.

Il principale è `/etc/httpd/conf/http.conf` che contiene tutti i parametri di configurazione del server WEB.

Alla fine dell'installazione si deve solo verificare che il servizio `httpd` sia attivo usando uno dei metodi visti in precedenza (`ntsysv` ad esempio).

I parametri di configurazione sono molteplici e si rimanda al sito www.apache.org per una lettura approfondita, poiché il server dopo l'installazione è già funzionante.

Di seguito si riportano i path delle cartelle principali usati di default:

<code>DocumentRoot /var/www/html/</code>	nella quale memorizzare le pagine Web,
<code>/cgi-bin /var/www/cgi-bin</code>	per i programmi cgi



Server FTP

In Fedora il server FTP utilizzato è **vsftp**.

Se già non è presente sul sistema si deve installare: `$ yum install vsftpd`

I file di configurazione si trovano nella directory `/etc/vsftpd`.

`/etc/vsftpd.conf` contiene tutti i parametri di configurazione del server ftp.

vsftpd permette il resume dei file, cioè la possibilità di riprendere il download dal punto in cui era stato interrotto.

La configurazione base non permette all'utente root di accedere in modalità ftp.

Questa limitazione è voluta per ragioni di sicurezza, infatti l'autenticazione degli utenti da parte del servizio ftp avviene "in chiaro", cioè login e password passano nella rete senza crittografia e sono leggibili con programmi di sniffing (tshark).

Alla fine dell'installazione si deve verificare che il servizio vsftpd sia attivo.

I parametri di configurazione sono molteplici e si rimanda alla pagina del manuale relativa: `man vsftpd` o `man vsftpd.conf`

Si consiglia di attivare il seguente parametro nel caso di un sistema usato da più utenti per evitare che possano leggere cartelle di livello superiore:

`chroot_list_enable=YES`

Di default Fedora usa SFTP un server FTP che usa il protocollo SSH per garantire la massima sicurezza, si consiglia di usare questo server.



Samba server

Il servizio **SAMBA** implementa sotto Linux il protocollo SMB di windows. SMB è un protocollo proprietario Microsoft che permette tra le altre funzionalità la condivisione di file e stampanti in una rete windows.

Si compone della parte client (per connettersi a condivisioni create in ambiente windows) e della parte server per condividere risorse Unix verso client windows.

I pacchetti da installare sono:

<code>yum install samba</code>	installa il server samba
<code>yum install samba-client</code>	installa il client di accesso alle condivisioni smb
<code>yum install samba-common</code>	installa software necessario sia al server che al client
<code>yum install system-config-samba</code>	installa il tool di configurazione grafico
<code>yum install samba-swat</code>	installa il tool di configurazione Web
<code>yum install smb4k</code>	installa il tool grafico di accesso alle condivisioni smb

`system-config-samba` permette una configurazione rapida del server: creazione di utenti e condivisione di file e cartelle.

`swat` permette di configurare sotto tutti gli aspetti il server samba, può essere utilizzato in alternativa alla modifica diretta del file di configurazione `/etc/samba/smb.conf`

Per attivare swat si deve usare `ntsysv` o `system-config-services` per indicare che il servizio deve essere attivo e poi riavviare il demone `xinetd`: `$ service xinetd restart`

Per usare swat è sufficiente aprire un comune browser e puntare all'indirizzo <http://sambaserver:901> (per l'accesso al server locale: <http://localhost:901>)



CUPS

La gestione delle stampanti in ambiente Linux ha subito un'evoluzione rapidissima. Dalla stampa gestita tramite il demone lpd nato quando esistevano le stampanti a caratteri, si è giunti alla nuova architettura CUPS (Common Unix Printing System).

CUPS implementa una gestione nuova della stampa con un'architettura modulare che permette di mantenere la compatibilità con i vecchi protocolli e una facile aggiunta di nuovi.

Supporta tra gli altri il protocollo IPP (Internet Printer Protocol) che permette di stampare attraverso internet garantendo una sicurezza elevata poichè usa un sistema di autenticazione e di crittografia.

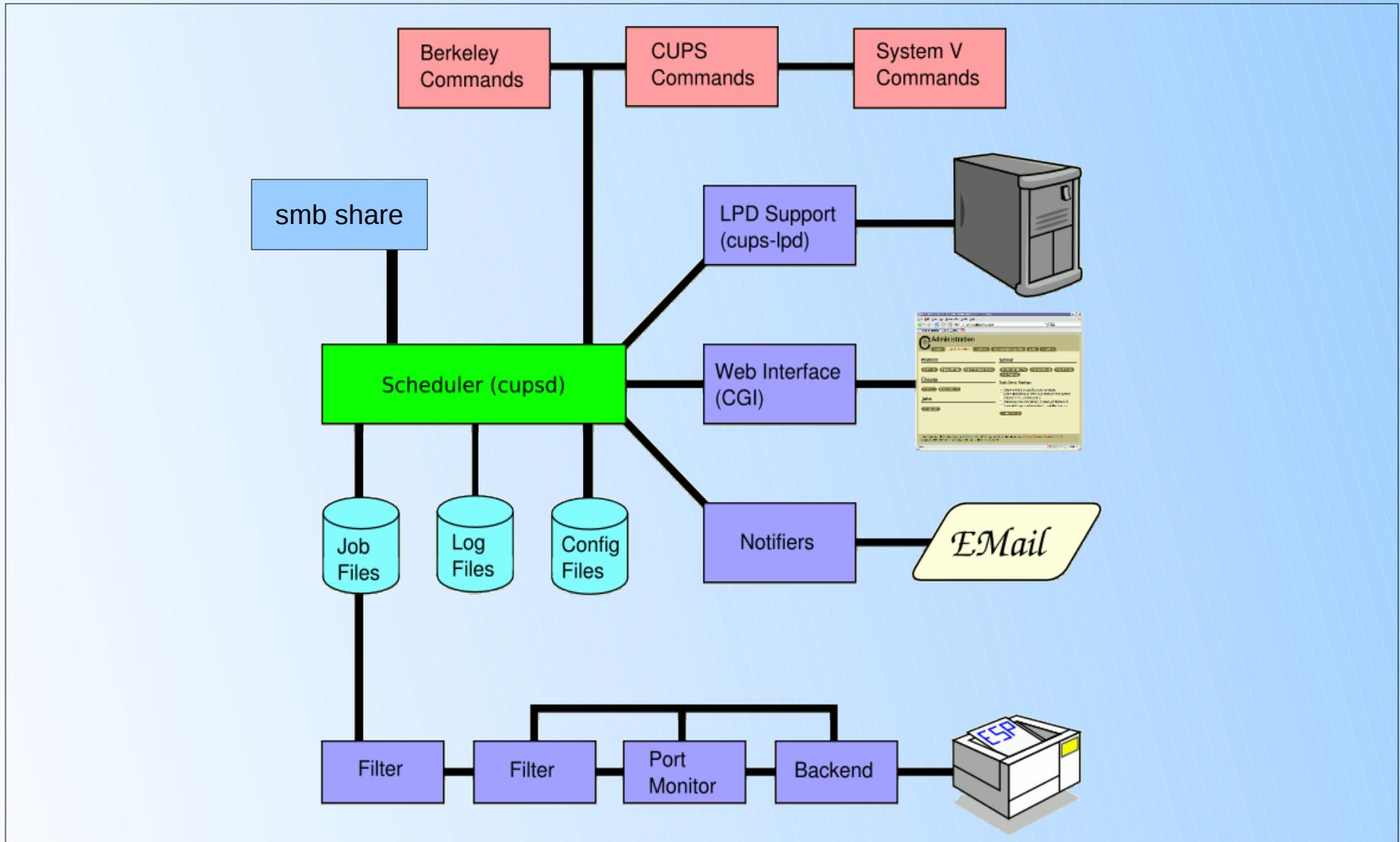
Per l'installazione è sufficiente digitare in una shell: `$ yum install cups`

La configurazione può essere effettuata tramite l'interfaccia Web disponibile al link: <http://localhost:631> in qualunque sistema sul quale sia installato CUPS.

Usando Fedora si può usare anche il tool: `system-config-printers`



CUPS architettura



NFS

Network File System

NFS è' un file system che permette la condivisione di directory tra computer connessi in rete.

Nel file di configurazione `/etc/exports` è riportata la ACL per il file system da condividere.

Sono elencate le directory condivise, gli host che le possono usare (montare) e le opzioni di condivisione.

Si basa sui servizi: `nfsd` e `mountd`

Ogni riga del file `exports` rappresenta un'esportazione ed ha la forma:
`<directory condivisa> host1(opzioni) [host2(opzioni)] ... [hostn(opzioni)]`

```
#sample file /etc/exports
/projects          proj*.local.domain(rw)
/home/joe          pc001(rw,all_squash,anonuid=150,anongid=100)
/srv/www           -sync,rw 192.168.1.0/24
```



Uso di condivisioni NFS

L'accesso alle condivisioni NFS oltre ad essere controllato dalla ACL presente nel file `/etc/exports` è legato ai permessi tipici dei file sotto Unix. E' importante quindi verificare i permessi e l'appartenenza del file ad utente e gruppo.

Per gestire le esportazioni di directory si può editare direttamente il file `/etc/exports` oppure utilizzare il front end grafico disponibile sotto Fedora: **system-config-nfs**

Se si apportano modifiche al file `exports` è necessario riavviare il servizio nfs:
`$ service nfs restart` oppure `/etc/inet.d/nfs restart`

Per usare i file system NFS condivisi su un pc remoto è necessario usare il comando `mount` alla pari di come si effettua il montaggio degli altri file system. Nel caso di condivisioni NFS il device sorgente va indicato nella forma:
`nome_host:/direcotry_condivisa`

E' possibile aggiungere il path NFS al file `/etc/fstab` per eseguire il mount al boot del sistema, ad esempio:

<nome_condivisione>	<punto di mount>	<tipo FS>	<opzioni>
<code>server:/path_remoto</code>	<code>/dir_locale</code>	<code>nfs</code>	<code>default 0 0</code>



Webmin

Per semplificare le operazioni di amministrazione e configurazione dei vari servizi disponibili in ambiente Linux, si consiglia di installare Webmin, un tool di configurazione con interfaccia Web.

Per la distribuzione Fedora 7 il pacchetto precompilato si trova aggiungendo un nuovo repository:

```
$ vi /etc/yum.repos.d/campworld.repo
```

```
[campworld]
```

```
name=CampWorld repo
```

```
baseurl=http://www.campworld.net/repos/FC7/
```

```
enabled=1
```

```
gpgcheck=0
```

```
yum install webmin
```

Per accedere al tool aprire il browser e puntare all'indirizzo: <https://localhost:10000>. Si ponga attenzione all'utilizzo del protocollo https che garantisce la massima sicurezza.

Questo tool presenta il grande vantaggio di permettere la configurazione remota di un server Linux, poichè l'interfaccia WEB (dopo aver configurato correttamente la security) è richiamabile da qualunque PC connesso in rete.



Corso Base su Linux

Fine Lezione 4

