Capitolo 36

Servizi di rete fondamentali

36.1 Supervisore dei servizi di rete

I servizi di rete vengono attivati all'avvio di un sistema GNU comune, attraverso la procedura di inizializzazione del sistema (Init), dopo che sono stati assegnati gli indirizzi alle interfacce di rete e dopo che gli instradamenti sono stati definiti.

I demoni in grado di fornire servizi di rete ricadono in due categorie possibili: autonomi (*standalone*) o gestiti dal supervisore dei servizi di rete, noto anche come *Internet service daemon*. Nel primo caso, si tratta di programmi avviati normalmente che si occupano si stare in ascolto su una certa porta e di provvedere da soli ai controlli necessari contro gli accessi indesiderati. Nel secondo, si tratta di programmi che vengono avviati nel momento in cui ne esiste effettivamente l'esigenza attraverso il supervisore dei servizi di rete, il quale si assume per loro il compito di rimanere in ascolto delle porte di accesso ai servizi che controlla.

La gestione «autonoma» è preferibile quando non è possibile attendere l'avvio di un programma ogni volta che si presenta una richiesta: il caso tipico è dato dal sistema di condivisione dei file system

in rete, o NFS. La gestione mediata dal supervisore dei servizi di rete permette di ridurre il carico del sistema, avviando solo i servizi necessari nel momento in cui ne viene fatta richiesta, introducendo eventualmente un controllo ulteriore per l'ammissibilità delle richieste pervenute.

36.1.1 Supervisore dei servizi di rete BSD

«

Ciò che realizza il concetto di supervisore dei servizi di rete è generalmente un programma sotto forma di demone, il quale può raccogliere su di sé tutte le funzionalità necessarie, oppure può affidarle in parte anche ad altre componenti. Il supervisore più comune è quello originario dei sistemi BSD, noto con il nome Inetd.[1]

Inetd, nella sua versione tradizionale dei sistemi BSD, non fa tutto il lavoro da solo, perché affida il controllo sull'ammissibilità degli accessi a quello che è noto come «TCP wrapper». Generalmente, Inetd si concretizza nel demone '**inetd**', mentre il TCP wrapper è costituito dal programma '**tcpd**'.

```
inetd [opzioni] [file_di_configurazione]
```

Di solito, il demone '**inetd**' viene avviato automaticamente dalla procedura di inizializzazione del sistema. Quando è in funzione, si mette in ascolto di un gruppo di porte determinato; quando rivela una comunicazione in una di queste, avvia il servizio corrispondente in base alla propria configurazione. In sostanza, questo demone demanda ad altri programmi specifici la gestione dei servizi richiesti.

La configurazione avviene attraverso il file '`/etc/inetd.conf`'; al suo interno sono indicati in particolare i programmi per la gestione

di servizi di rete specifici. In molti casi, l'avvio di questi programmi viene sottoposto al controllo del TCP wrapper, ovvero di '**tcpd**'. Se si fanno modifiche a questo file e si vuole che abbiano effetto, è necessario inviare a '**inetd**' un segnale di aggancio, ovvero '**SIGHUP**':

```
kill -HUP pid_di_inetd
```

Sotto viene mostrato il contenuto tipico di questo file, così come appare nelle distribuzioni GNU più comuni. La prima cosa da osservare è che il simbolo '**#**', posto all'inizio di una riga, introduce un commento; inoltre, le righe bianche e quelle vuote vengono ignorate. Tutte le altre righe vengono interpretate come direttive di dichiarazione di un servizio particolare.

```
#echo          stream  tcp     nowait  root    internal
#echo          dgram   udp     wait    root    internal
#chargen       stream  tcp     nowait  root    internal
#chargen       dgram   udp     wait    root    internal
discard        stream  tcp     nowait  root    internal
discard        dgram   udp     wait    root    internal
daytime        stream  tcp     nowait  root    internal
#daytime       dgram   udp     wait    root    internal
time           stream  tcp     nowait  root    internal
#time          dgram   udp     wait    root    internal

telnet  stream  tcp     nowait  root    /usr/sbin/tcpd /usr/sbin/telnetd
telnets stream  tcp     nowait  root    /usr/sbin/tcpd /usr/sbin/telnetd
ident   stream  tcp     nowait  root    /usr/sbin/ident2        ident2
rsync   stream  tcp     nowait  root    /usr/bin/rsync rsyncd --daemon
```

Per l'utente medio di un sistema GNU non è necessario approfondire la sintassi di queste direttive in quanto il file viene prodotto automaticamente dagli script di installazione dei pacchetti, corrispondenti ai

servizi che si intendono gestire. Tuttavia, quando si vuole avere un controllo maggiore del proprio sistema operativo, la configurazione manuale di questo file non può essere evitata.

Le direttive di questo file sono dei record, corrispondenti in pratica alle righe, suddivisi in campi distinti attraverso spaziature orizzontali (spazi o tabulazioni). L'ultimo campo può contenere anche spazi.

servizio [**/** ***versione***] ***tipo_socket*** ***protocollo*** { `wait` | `nowait` } [**.** ***max***] ↩
↪***utente*** [**.** ***gruppo***] ***programma_del_servizio*** ***programma_e_argomenti***

1. ***servizio*** [**/** ***versione***]

   Il primo campo serve a indicare il servizio. Normalmente si fa riferimento a una porta indicata per nome, secondo quanto definito dal file '`/etc/services`'. Se si indica un numero, si fa riferimento direttamente a quel numero di porta.

   Eventualmente può essere indicato un servizio RPC; in tal caso si utilizza un nome secondo quanto riportato nel file '`/etc/rpc`', seguito eventualmente da un barra obliqua e dal numero di versione.

2. ***tipo_socket***

   Definisce il tipo di socket attraverso diverse parole chiave:

   - '**`stream`**'
   - '**`dgram`**' datagramma
   - '**`raw`**'

- '**rdm**' *reliably delivered message*
- '**seqpacket**' *sequenced packet socket*

3. ***protocollo***

   Serve a determinare il tipo di protocollo, utilizzando una parola chiave che si ottiene dal file '`/etc/protocols`'. Si tratta prevalentemente di '**tcp**' e '**udp**'. Nel caso si vogliano gestire protocolli RPC, questi si indicano come '**rpc/tcp**' e '**rpc/udp**'.

   Tuttavia c'è un'eccezione, dovuta alla distinzione tra richieste di tipo IPv4 e IPv6: quando si fa riferimento a un protocollo TCP o UDP, le sigle '**tcp**' e '**udp**' si riferiscono alla versione predefinita (inizialmente quella di IPv4). Per poter gestire sia IPv4, sia IPv6, occorre indicare precisamente le sigle '**tcp4**' e '**udp4**', oppure '**tcp6**' e '**udp6**'. Pertanto, supponendo che un certo servizio possa operare sia con IPv4, sia con IPv6, le voci corrispondenti nel file di configurazione si raddoppiano. L'esempio successivo ipotizza un servizio TELNET, realizzato attraverso il programma '**telnetd**', in grado di operare sia con IPv4, sia con IPv6:

```
telnet stream tcp4 nowait root /usr/sbin/tcpd /usr/sbin/telnetd
telnet stream tcp6 nowait root /usr/sbin/tcpd /usr/sbin/telnetd
```

4. { *wait* | *nowait* } [. *max*]

   Le parole chiave '**wait**' e '**nowait**' servono a definire il comportamento di un servizio, quando si utilizza il tipo di socket '**dgram**' (datagramma). In tutti gli altri casi, si usa esclusivamente la parola chiave '**nowait**'.

In base alle richieste dei clienti, il demone '**inetd**' può avviare un certo numero (anche elevato) di copie di processi di uno stesso servizio. Il limite predefinito è di 40 ogni minuto (ovvero ogni 60 secondi) e può essere modificato aggiungendo alla parola chiave '**wait**' o '**nowait**' un'estensione composta da un punto seguito da un numero: il numero massimo di copie per minuto.

5. *utente* [*.gruppo*]

Serve a definire l'utente ed eventualmente il gruppo in nome del quale avviare il servizio. Inetd viene avviato dalla procedura di inizializzazione del sistema, con i privilegi dell'utente '**root**'; di conseguenza, può cambiare l'utente e il gruppo proprietari dei processi che avvia, in modo da dare loro i privilegi strettamente necessari al compimento delle loro funzioni.

6. *programma_del_servizio*

Definisce il percorso assoluto di avvio del programma che offre il servizio. Se si tratta di un servizio interno al supervisore dei servizi di rete stesso, si utilizza la parola chiave '**internal**' e l'ultimo campo non viene indicato.

7. *programma_e_argomenti*

L'ultimo campo è anomalo, in quanto consente l'utilizzo degli spazi come parte dell'informazione in esso contenuta: si tratta del nome del programma, senza percorso, seguito dagli argomenti eventuali con cui questo deve essere avviato. Si osservi l'esempio

seguente, in cui ci si trova a dover ripetere il nome ‘**ident2**’ per questo motivo:

```
…
ident   stream  tcp   nowait  root   /usr/sbin/ident2  ident2
…
```

36.1.2 TCP wrapper

L’avvio di alcuni servizi può essere controllato utilmente da un sistema di registrazione e verifica, separato da Inetd, definito TCP wrapper.[2] Si tratta di un programma, o di una libreria da inserire in un programma che offre qualche tipo di servizio, con cui si eseguono dei controlli, in base ai quali si decide se avviare o meno il servizio corrispondente. Il TCP wrapper non è indispensabile per Inetd, ma il suo utilizzo è diventato una consuetudine, per poter avere almeno un controllo minimo sui servizi principali.

I compiti del TCP wrapper possono essere: annotare le connessioni nel registro di sistema; filtrare l’accesso ai servizi in base a regole determinate; eseguire delle verifiche contro possibili «imbrogli»; utilizzare protocolli di identificazione dell’utente da cui ha origine la richiesta di accesso.

Come accennato, può trattarsi di un programma generalizzato, come nel caso del demone ‘**tcpd**’, oppure di una libreria che normalmente viene utilizzata dai programmi che funzionano in modo indipendente dal supervisore dei servizi di rete.

Qui viene mostrato solo l’uso elementare del TCP wrapper; tuttavia, si deve considerare che le funzionalità effettivamente disponibili dipendono anche dal modo in cui questo è stato compilato.

Per un approfondimento delle sue potenzialità, si può consultare la documentazione originale: *tcpd(8)* e *hosts_access(5)*; inoltre, nella sezione 43.4 viene descritto come si può usare per realizzare delle «trappole».

La configurazione del TCP wrapper avviene attraverso la coppia di file '`/etc/hosts.allow`' e '`/etc/hosts.deny`'. Semplificando, quando il TCP wrapper viene interpellato a proposito di un tentativo di accesso, questo verifica che l'indirizzo del chiamante sia incluso nell'elenco di '`/etc/hosts.allow`'. Se è così non esegue altri controlli e permette l'accesso, altrimenti verifica che questo non sia incluso nell'elenco di '`/etc/hosts.deny`' (se entrambi i file mancano o sono vuoti, sono consentiti tutti gli accessi).

36.1.3 Dichiarazione all'interno di «/etc/inetd.conf»

«

La dichiarazione di un servizio all'interno del file '`/etc/inetd.conf`' (relativo a Inetd) può avvenire fondamentalmente in due modi possibili: con o senza il filtro del TCP wrapper. Si osservino i due esempi seguenti.

```
…
telnet  stream  tcp  nowait  root  /usr/sbin/in.telnetd  ↩
↪in.telnetd
…
```

```
…
telnet  stream  tcp  nowait  root /usr/sbin/tcpd  in.telnetd
…
```

Nel primo caso, quando si instaura una connessione TELNET, il supervisore dei servizi di rete avvia direttamente il binario

‘`/usr/sbin/in.telnetd`’, senza altre intermediazioni. L’albero dei processi potrebbe apparire come nell’esempio seguente:

```
$ pstree [Invio]

  init-+-inetd---in.telnetd---login---bash---…
       |
       …
```

Nel secondo caso, invece, un’eventuale connessione TELNET viene preceduta dalla verifica attraverso il TCP wrapper (in questo caso, costituito dal programma ‘**`tcpd`**’), il quale potrebbe anche rifiutarla, oppure semplicemente aggiungere dei controlli. Ma una volta completati i controlli, se il servizio può essere avviato, il programma ‘**`tcpd`**’ si toglie di mezzo, per cui l’albero dei processi appare esattamente uguale a quanto già visto.

Quando si decide di utilizzare il TCP wrapper, si possono presentare altre possibilità. Per la precisione, perché funzioni quanto visto nell’ultimo esempio, occorre che l’eseguibile ‘**`in.telnetd`**’ si trovi nella directory prevista dal programma ‘**`tcpd`**’, secondo quanto definito in fase di compilazione dei sorgenti. In pratica, per un sistema GNU si tratta di ‘`/usr/sbin/`’.

Se il demone di un servizio determinato si trova in una collocazione differente rispetto a quella standard, questo potrebbe essere indicato utilizzando il percorso assoluto, come nell’esempio seguente:

```
…
telnet  stream  tcp  nowait  root  /usr/sbin/tcpd ↩
↪/root/bin/in.telnetd
…
```

In questo caso, viene specificato che il demone necessario a ri-

cevere le connessioni TELNET è precisamente '`/root/bin/in.telnetd`'.

36.1.4 Configurazione del TCP wrapper

«

Come già accennato, la configurazione del TCP wrapper avviene attraverso la coppia di file '`/etc/hosts.allow`' e '`/etc/hosts.deny`', dove il primo serve a individuare accessi consentiti, mentre il secondo serve a definire accessi non consentiti.

I tentativi di accesso sono confrontati con le direttive contenute nel file '`/etc/hosts.allow`', continuando eventualmente con quelle di '`/etc/hosts.deny`'. Se si ottiene una corrispondenza con una direttiva del file '`/etc/hosts.allow`', l'accesso viene concesso, senza passare al controllo di '`/etc/hosts.deny`'; se non si ottiene alcuna corrispondenza con le direttive del file '`/etc/hosts.allow`', si passa all'analisi di quelle contenute in '`/etc/hosts.deny`' e solo se nessuna corrisponde all'accesso in corso, questo viene consentito. Pertanto, se i file '`/etc/hosts.allow`' e '`/etc/hosts.deny`' sono vuoti, o mancano, sono consentiti tutti gli accessi.

In generale, le righe che iniziano con il simbolo '**#**' sono ignorate, in qualità di commenti; le righe bianche e quelle vuote sono ignorate ugualmente. Le direttive occupano normalmente una riga, a meno che terminino con il simbolo '****' (subito prima del codice di interruzione di riga) che rappresenta una continuazione nella riga successiva.

La sintassi minima per le direttive di questi file dovrebbe corrisponde allo schema seguente:

```
elenco_di_demoni : elenco_di_clienti
```

Alla sinistra dei due punti si elencano i programmi demone il cui utilizzo si vuole concedere ai nodi di rete elencati alla destra. Gli elementi appartenenti a un elenco possono essere separati con una virgola o uno spazio.

È consentito l'uso di speciali nomi in qualità di metavariabili e altri simboli che facilitano l'indicazione di gruppi di nomi. Segue un elenco di elementi utilizzabili.

Elemento	Descrizione
.indirizzo_ipv4 *.nome_a_dominio*	L'indirizzo IPv4 di un nodo che inizia con un punto indica in realtà tutti gli indirizzi che finiscono con quel suffisso. Se si utilizzano nomi a dominio invece di indirizzi numerici, si fa riferimento a un intero dominio. Per esempio, '`.brot.dg`' rappresenta tutti i nodi del dominio *brot.dg*.
indirizzo_ipv4 . *prefisso_nome_a_dominio* .	L'indirizzo di un nodo che finisce con un punto indica in realtà tutti gli indirizzi che iniziano con quel prefisso. Se si utilizzano indirizzi IPv4 numerici, si fa riferimento a una rete intera. Per esempio, '`192.168.`' rappresenta tutti i nodi della rete 192.168.0.0.

Elemento	Descrizione
`@`***dominio_nis***	Il nome di un dominio NIS viene indicato con il prefisso '`@`' e rappresenta tutti i nodi che appartengono a tale dominio.
indirizzo_ipv4 / ***maschera_ipv4***	Rappresenta gli indirizzi IPv4 che si ottengono eseguendo l'AND tra indirizzo e maschera. Per esempio, 192.168.72.0/255.255.254.0 rappresenta tutti gli indirizzi a partire da 192.168.72.0 a 192.168.73.255.
`[`***indirizzo_ipv6***`]` / ***n_bit_maschera***	Rappresenta un gruppo di indirizzi IPv6, secondo la maschera. Per esempio, '`[fec0:0:0:1::]/64`' rappresenta tutti gli indirizzi fec0:0000:0000:0001::.
`ALL`	È una metavariabile che rappresenta tutto. Se si trova alla sinistra dei due punti indica tutti i demoni dei servizi, se si trova alla destra rappresenta tutti i nodi.
`LOCAL`	È una metavariabile che indica tutti gli elaboratori locali, intendendosi con questo quelli rappresentabili senza alcun punto.

Elemento	Descrizione
`UNKNOWN`	È una metavariabile che rappresenta tutti i nodi il cui nome o indirizzo risulta sconosciuto. Se si vuole usare questo modello, occorre considerare che i nodi potrebbero risultare sconosciuti anche a causa di un'interruzione temporanea del servizio DNS.
`KNOWN`	È una metavariabile che rappresenta tutti i nodi il cui nome o indirizzo risulta conosciuto. Se si vuole usare questo modello, occorre considerare che i nodi potrebbero risultare sconosciuti anche a causa di un'interruzione temporanea del servizio DNS.
`PARANOID`	È una metavariabile che corrisponde ai nodi il cui nome non corrisponde all'indirizzo. In pratica, si vuole che '**`tcpd`**', attraverso il DNS, determini l'indirizzo in base al nome, quindi si vuole ancora che trasformi il nome in indirizzo (indirizzo --> nome --> indirizzo); se non c'è corrispondenza tra gli indirizzi ottenuti, il nodo rientra in questa categoria.
`EXCEPT`	È un operatore che può essere utilizzato all'interno di un elenco di nomi per escluderne i successivi.

Segue un elenco di esempi riferiti a direttive del file ‘`/etc/hosts.allow`’:

Esempio	Descrizione
`ALL : ALL`	Consente l’utilizzo di qualsiasi servizio da parte di qualsiasi nodo.
`ALL : ALL EXCEPT .mehl.dg`	Consente l’utilizzo di qualsiasi servizio da parte di qualsiasi nodo a eccezione di quelli il cui dominio è *mehl.dg*.
`ALL : .brot.dg`	Consente l’utilizzo di qualsiasi servizio da parte dei nodi appartenenti al dominio *brot.dg*.
`ALL : .brot.dg EXCEPT caino.brot.dg`	Consente l’utilizzo di qualsiasi servizio da parte dei nodi appartenenti al dominio *brot.dg*, a esclusione di *caino.brot.dg*.
`ALL : 192.168.`	Consente l’utilizzo di qualsiasi servizio da parte dei nodi appartenenti alla sottorete 192.168.0.0.

Esempio	Descrizione
`in.fingerd : LOCAL` `ALL : ALL`	L'ordine in cui appaiono le direttive è importante. In questo caso, le richieste per il servizio Finger (rappresentato dal demone '**`in.fingerd`**'), vengono accettate solo se provengono da indirizzi locali. Tutti gli altri servizi sono permessi da qualunque origine.

Per un controllo più facile degli accessi, conviene indicare all'interno del file '`/etc/hosts.deny`' soltanto '**`ALL : ALL`**' in modo da impedire tutti gli accessi che non siano consentiti esplicitamente da '`/etc/hosts.allow`'.

36.2 RPC: Remote Procedure Call

RPC, acronimo di *Remote procedure call*, è un meccanismo generale per la gestione di applicazioni cliente-servente. Il sistema si basa su un demone, il Portmapper, e un file che elenca i servizi disponibili associati al demone relativo. Il Portmapper funziona in modo autonomo dal supervisore dei servizi di rete. Semplificando in modo estremo il funzionamento delle RPC, si può dire che si tratti di un meccanismo attraverso cui si possono eseguire delle elaborazioni remote.

Dal lato servente si trova il Portmapper[3] in ascolto sulla porta 111, dal lato cliente ci sono dei programmi che, per un servizio RPC qua-

lunque, devono prima interpellare il Portmapper remoto per ottenere le informazioni necessarie a stabilire una connessione con il demone competente.

Per questo motivo, le chiamate RPC contengono l'indicazione di un ***numero di programma***, attraverso il quale, il Portmapper remoto è in grado di rispondere informando il cliente sul numero di porta da utilizzare per quel programma.

I servizi RPC possono essere interrogati attraverso il programma '**rpcinfo**'. Per esempio, per chiedere al Portmapper dell'elaboratore *weizen.mehl.dg* quali servizi sono disponibili e per conoscere le loro caratteristiche, si può agire come nell'esempio seguente:

```
$ rpcinfo -p weizen.mehl.dg[Invio]

   program vers proto   port
    100000    2   tcp    111  portmapper
    100000    2   udp    111  portmapper
    100005    1   udp    844  mountd
    100005    1   tcp    846  mountd
    100003    2   udp   2049  nfs
    100003    2   tcp   2049  nfs
```

Una cosa da osservare è che alcuni dei programmi elencati tra i servizi RPC, non appaiono necessariamente anche nell'elenco del file '`/etc/services`'.

Il demone che si occupa di attivare i servizi RPC è '**portmap**' (a volte anche '**rpc.portmap**'), avviato e fermato dalla procedura di inizializzazione del sistema (restando indipendente dal controllo del supervisore dei servizi di rete).

```
portmap [opzioni]
```

Il file ‘/etc/rpc’ contenente l’elenco dei servizi RPC disponibili, abbinati al numero di programma usato come riferimento standard. Il suo scopo è quindi quello di tradurre i nomi in numeri di programma e viceversa. Questi numeri riguardano esclusivamente la gestione dei servizi RPC e non vanno confusi con i numeri di porta (TCP/UDP ‘/etc/services’) o di protocollo (IP ‘/etc/protocols’).

```
# This file contains user readable names that can be used
# in place of rpc program numbers.
portmapper      100000  portmap sunrpc
rstatd          100001  rstat rstat_svc rup perfmeter
rusersd         100002  rusers
nfs             100003  nfsprog
ypserv          100004  ypprog
mountd          100005  mount showmount
ypbind          100007
walld           100008  rwall shutdown
yppasswdd       100009  yppasswd
etherstatd      100010  etherstat
rquotad         100011  rquotaprog quota rquota
…
```

36.2.1 Informazioni sulle RPC

Per interrogare un Portmapper si utilizza normalmente il programma ‘**rpcinfo**’:[4]

```
rpcinfo -p [nodo]
```

```
rpcinfo [-n numero_di_porta] {-u|-t} nodo programma [versione]
```

```
rpcinfo {-b|-d} programma versione
```

L'utilità di questo programma sta quindi nella possibilità di conoscere quali servizi RPC sono disponibili all'interno di un certo nodo, oltre alla possibilità di verificare che questi siano effettivamente in funzione.

Tabella 36.12. Alcune opzioni.

Opzione	Descrizione
`-p` [*nodo*]	Interroga il Portmapper nell'elaboratore indicato, oppure in quello locale, elencando tutti i programmi RPC registrati presso lo stesso.
`-u` *nodo programma* [*versione*]	Utilizza il protocollo UDP per eseguire una chiamata RPC alla procedura zero ('**NULLPROC**') del programma nel nodo specificato. Il risultato viene emesso attraverso lo standard output.
`-t` *nodo programma* [*versione*]	Utilizza il protocollo TCP per eseguire una chiamata RPC alla procedura zero ('**NULLPROC**') del programma nel nodo specificato. Il risultato viene emesso attraverso lo standard output.
`-n` *numero_di_porta*	Permette di specificare una porta diversa rispetto a quella che viene indicata dal Portmapper, per eseguire una chiamata RPC attraverso le opzioni '**-u**' e '**-t**'.

Opzione	Descrizione
`-b` ***programma versione***	Permette di eseguire una chiamata RPC circolare (broadcast) a tutti i nodi in grado di riceverla, utilizzando il protocollo UDP, per l'esecuzione della procedura zero ('**`NULLPROC`**') del programma e della versione specificati. Il risultato viene emesso attraverso lo standard output.
`-d` ***programma versione***	L'utente '**`root`**' può utilizzare questa opzione per eliminare la registrazione del servizio RPC del programma e della versione specificati.

Seguono alcuni esempi:

`$` **`rpcinfo -p`** [*Invio*]

Elenca tutti i servizi RPC registrati nell'elaboratore locale.

```
   program vers proto   port
    100000    2   tcp    111  portmapper
    100000    2   udp    111  portmapper
    100005    1   udp    844  mountd
    100005    1   tcp    846  mountd
    100003    2   udp   2049  nfs
    100003    2   tcp   2049  nfs
```

`$` **`rpcinfo -p weizen.mehl.dg`** [*Invio*]

Elenca tutti i servizi RPC registrati nell'elaboratore *weizen.mehl.dg*.

`$` **`rpcinfo -b mountd 1`** [*Invio*]

Elenca tutti i nodi in grado di fornire il servizio '**`mountd`**'.

```
127.0.0.1 localhost.localdomain
192.168.1.1 dinkel.brot.dg
192.168.1.2 roggen.brot.dg
```

36.2.2 Controllo sulle RPC

«

Generalmente, il Portmapper non viene messo sotto il controllo del supervisore dei servizi di rete; tuttavia, potrebbe essere stato compilato in modo da tenere in considerazione il contenuto dei file '`/etc/hosts.allow`' e '`/etc/hosts.deny`'. Indipendentemente dal fatto che ciò sia vero, se si usano questi file conviene prevedere le direttive che riguardano il Portmapper, in vista di aggiornamenti futuri. In generale, conviene inserire nel file '`/etc/hosts.allow`' la riga seguente:

```
portmap: specifica_dei_nodi
```

Per converso, conviene indicare la riga seguente nel file '`/etc/hosts.deny`', allo scopo di escludere gli accessi che non provengano dai nodi autorizzati espressamente:

```
portmap: ALL
```

Eventualmente, per una sicurezza maggiore, può essere conveniente inserire soltanto la direttiva seguente nel file '`/etc/hosts.deny`', sapendo che questa interferisce però con tutti gli altri programmi che interpretano questi file:

```
ALL: ALL
```

Ai fini del controllo attraverso filtri di pacchetto che si basano sul riconoscimento delle porte TCP o UDP, va ricordato che il Portmapper utilizza solitamente la porta 111.

36.3 NFS con i sistemi GNU/Linux

NFS è un servizio di rete che, avvalendosi delle RPC, permette la condivisione di porzioni di file system da e verso altri elaboratori connessi. Nell'ambito del modello ISO-OSI, il protocollo NFS si colloca al livello cinque (sessione). A seconda della versione del protocollo NFS, questo può avvalersi, al livello sottostante (trasporto), del protocollo UDP o del protocollo TCP.

Per la gestione o l'utilizzo del servizio NFS, il kernel Linux deve incorporare del codice appropriato che nella procedura di configurazione si individua come facoltà di gestione del file system NFS (sezione 8.3.9); tuttavia, benché incorporate, tali funzionalità devono poi essere controllate attraverso programmi di contorno.

Si può verificare la possibilità di accedere a un file system NFS leggendo il contenuto del file '`/proc/filesystems`'. L'esempio seguente rappresenta una situazione in cui ciò è possibile, per la presenza della riga '**`nodev nfs`**':

```
        ext3
        ext2
        minix
        umsdos
        msdos
        vfat
nodev   proc
nodev   nfs
nodev   smbfs
        iso9660
```

Per scoprire se il kernel consente di gestire la funzionalità di servente NFS, si può cercare il file '`/proc/net/rpc/nfsd`', il quale potrebbe contenere qualcosa simile all'esempio seguente:

```
rc 0 63064 138528
fh 0 194531 0 0 0
io 61203811 330360802
th 8 350 47.860 3.570 1.470 0.000 0.880 0.730 0.250 ↩
↪0.290 0.000 1.760
ra 16 7654 169 54 60 23 53 24 14 20 21 2115
net 201592 201592 0 0
rpc 201592 0 0 0 0
proc2 18 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
proc3 22 2 771 4595 101428 13065 19 10207 51228 3301 ↩
↪16 34 0 3310 15 520 45 2130 0 45 45 0 10816
```

36.3.1 Dal lato del servente

«

Dalla parte dell'elaboratore servente è necessario che oltre al Portmapper siano in funzione alcuni demoni, avviati secondo l'ordine seguente: '**rpc.mountd**', '**rpc.nfsd**', '**rpc.statd**', '**rpc.lockd**' ed eventualmente '**rpc.rquotad**'.[5] Quindi, è necessario che il file di configurazione '/etc/exports' sia stato configurato correttamente. Si può controllare la presenza del servizio attraverso l'interrogazione delle RPC:

```
$ rpcinfo -p [Invio]
```

```
    program vers proto   port
     100000    2   tcp    111  portmapper
     100000    2   udp    111  portmapper
     100024    1   udp  54407  status
     100024    1   tcp  38826  status
     100003    2   udp   2049  nfs
     100003    3   udp   2049  nfs
     100021    1   udp  54411  nlockmgr
     100021    3   udp  54411  nlockmgr
     100021    4   udp  54411  nlockmgr
     100005    1   udp  54412  mountd
     100005    1   tcp  38827  mountd
     100005    2   udp  54412  mountd
     100005    2   tcp  38827  mountd
     100005    3   udp  54412  mountd
     100005    3   tcp  38827  mountd
```

Nello stesso modo, si può analizzare l'albero dei processi:

```
$ pstree [Invio]

  init-+-…
       …
        |-lockd---rpciod
       …
        |-8*[nfsd]
       …
        |-portmap---portmap
       …
        |-rpc.mountd
        |-rpc.statd
       …
```

Il programma '**rpc.mountd**' è il demone che si occupa di gestire l'innesto del file system di rete dal lato del servente:

```
rpc.mountd [opzioni]
```

Generalmente, viene avviato dalla procedura di inizializzazione del sistema, in modo autonomo, cioè indipendente dal supervisore dei servizi di rete. Mantiene aggiornato il file '`/var/lib/nfs/rmtab`' che elenca gli innesti in essere. Tuttavia, non è garantito che il contenuto di questo file sia esatto, per cui non lo si può utilizzare per determinare con certezza quali siano le connessioni in corso.

Il programma '**`rpc.nfsd`**' è il demone che si occupa di gestire le richieste, da parte dei clienti, per i servizi NFS, avvalendosi in pratica delle funzionalità del kernel Linux.

```
rpc.nfsd [opzioni]
```

Deve essere in funzione nel servente. Viene avviato generalmente dalla procedura di inizializzazione del sistema, subito dopo '**`rpc.mountd`**'. Anche '**`rpc.nfsd`**' funziona in modo autonomo rispetto al supervisore dei servizi di rete.

Il demone '**`rpc.lockd`**' si occupa di avviare la gestione del sistema di file lucchetto NFS, noto come NLM, ovvero *NFS lock manager*:

```
rpc.lockd
```

In generale, con i kernel Linux recenti non dovrebbe essere necessaria la presenza di questo programma; tuttavia, anche se così fosse, il suo avvio non provoca inconvenienti.

Il demone '**`rpc.statd`**' serve al sistema di file lucchetto NFS

per aggiornare la situazione quando un elaboratore cliente viene riavviato o comunque si blocca:

```
rpc.statd [opzioni]
```

La configurazione del servizio avviene principalmente attraverso il file '`/etc/exports`', il quale contiene l'indicazione delle porzioni di file system locale da concedere in condivisione. Se il file manca o è vuoto, non viene concesso l'utilizzo di alcuna parte del file system locale all'esterno.

Si tratta di un file di testo normale, in cui vengono ignorate le righe vuote, quelle bianche e quelle che iniziano con il simbolo '**#**'; per il resto, le righe sono intese come dei record, ognuno dei quali è composto da:

- l'indicazione di una directory a partire dalla quale si concede la condivisione;
- una serie di nodi o reti cui viene concesso l'utilizzo di questa directory con l'eventuale specificazione di opzioni di accesso.

In pratica si utilizza la sintassi seguente:

```
directory_di_partenza [nodo] [(opzioni)] ...
```

La configurazione di questo file potrebbe non dare sempre gli effetti previsti, a causa di difetti che possono essere presenti nei demoni che si occupano della gestione del servizio. In generale, si è cercato sempre di garantire la sicurezza, a discapito della funzionalità. Se una configurazione di '`/etc/exports`' sembra non funzionare senza un motivo apparente, è bene provarne altre, limitando l'uso di opzioni particolari, o cercando di identificare meglio gli elaboratori a cui si concede l'accesso. Eventualmente, si veda anche la pagina di manuale *exports(5)*.

Gli elaboratori a cui si concede l'accesso alla directory condivisa possono essere specificati in vari modi, alcuni dei quali sono elencati di seguito:

- **indicazione di un nodo singolo**

  quando si utilizza un nome o un indirizzo IP che fa riferimento da un elaboratore specifico;

- **uso di caratteri jolly**

  possono essere utilizzati i caratteri jolly '`*`' e '`?`' per indicare un gruppo di **nomi** di elaboratore con una sola notazione, tenendo presente che questi simboli non possono sostituirsi ai punti di un nome a dominio;

- **rete IP**

  attraverso la notazione '***indirizzo_ip / maschera_di_rete***' è possibile indicare simultaneamente tutti gli elaboratori collocati all'interno della rete o della sottorete a cui si fa riferimento.

Le opzioni tra parentesi tonde sono parole chiave particolari. Segue la descrizione di alcune di queste:

Parola chiave	Descrizione
`ro`	Consente l'accesso in sola lettura. Questa è la modalità di funzionamento predefinita.
`rw`	Consente l'accesso in lettura e scrittura.

`insecure_lock`
 	
`no_auth_nlm`
	Questa opzione consente di usare un sistema di file lucchetto meno rigido, quando alcuni elaboratori clienti mostrano difficoltà in questo senso.

`root_squash`	Si tratta di un'opzione di sicurezza, di solito predefinita, attraverso la quale si impedisce l'accesso come utente '**`root`**'. In pratica, quando un utente '**`root`**' presso un elaboratore cliente utilizza il file system condiviso, viene trattato come utente '**`nobody`**'. L'utente '**`nobody`**' corrisponde spesso al numero UID 65534 (o −2 se si vuole considerare il valore come intero a 16 bit); tuttavia, questo utente non ha un numero UID standard, tanto che in alcuni sistemi si preferisce utilizzare un numero più basso di quelli assegnati agli utenti comuni.
`all_squash`	La presenza di questa opzione fa sì che tutti gli accessi al file system condiviso, avvengano con i privilegi dell'utente '**`nobody`**'.

Parola chiave	Descrizione
`no_root_squash`	Non effettua la trasformazione dell'UID '**`root`**' e ciò è necessario quando si utilizzano clienti NFS senza disco fisso. Tuttavia, per mitigare il problema di sicurezza che si crea inevitabilmente, è auspicabile che l'uso di questa opzione sia abbinato almeno a un accesso in sola lettura.

L'elenco seguente mostra alcuni esempi di record di questo file; tuttavia si ricordi che tutto va verificato con il proprio kernel e con la versione del protocollo NFS usati effettivamente.

Esempio	Descrizione
`/usr *.brot.dg(ro)`	Concede ai nodi del dominio *brot.dg* l'accesso in lettura alla directory '`/usr/`' e seguenti.
`/ roggen.brot.dg(ro,root_squash)`	Concede a *roggen.brot.dg* di accedere in sola lettura a partire dalla directory radice, escludendo i privilegi dell'utente '**`root`**'.
`/home roggen.brot.dg(rw) weizen.mehl.dg(rw)`	Concede a *roggen.brot.dg* e a *weizen.mehl.dg* di accedere in lettura e scrittura alla directory '`/home/`'.

Esempio	Descrizione
`/usr/local 192.168.0.0/255.255.0.0(ro)`	Concede a tutti i nodi con indirizzi 192.168.*.* di accedere in lettura a partire dalla directory '`/usr/local/`'.
`/usr/local 192.168.0.0/16(ro)`	Esattamente come nell'esempio precedente, con una rappresentazione compatta della maschera di rete.
`/ *(ro,no_root_squash)`	Questa definizione non dovrebbe funzionare. Sembrerebbe voler concedere a tutta la rete di accedere in lettura a partire dalla directory radice, permettendo ai vari utenti '**`root`**' di mantenere i loro privilegi. Tuttavia l'asterisco non dovrebbe riuscire a rimpiazzare i punti che compongono i nomi a dominio, risolvendosi così in una directory che in pratica non viene condivisa.

Esempio	Descrizione
`/ 0.0.0.0/0(ro,no_root_squash)`	Teoricamente, questo dovrebbe essere il modo corretto per ottenere il risultato che si presume voler ottenere nell'esempio precedente, limitatamente ai nodi con indirizzi IPv4.

Quando si modifica il file '`/etc/exports`', per garantire che il suo aggiornamento sia preso in considerazione dal sistema di condivisione del file system, è necessario utilizzare il programma '**`exportfs`**' nel modo seguente:

```
# exportfs -ra [Invio]
```

Il programma '**`exportfs`**' può anche essere usato per esportare al volo una directory, senza modificare il file '`/etc/exports`'. In generale, si tratta di una pratica non consigliabile, ma della quale bisogna tenere conto. Eventualmente si può consultare la pagina di manuale *exportfs(8)*.

Infine, bisogna considerare che alcuni dei demoni che abilitano il servizio NFS potrebbero essere stati compilati in modo da utilizzare i file '`/etc/hosts.allow`' e '`/etc/hosts.deny`' per controllare l'accesso. L'elenco seguente mostra in che modo abilitare o disabilitare l'accesso in modo selettivo per ogni demone coinvolto, tenendo conto che anche il Portmapper potrebbe dipendere da questi file:

Demone	‘/etc/hosts.allow’	‘/etc/hosts.deny’
Portmapper	`portmap:` ***specifica_dei_nodi***	`portmap:` ***specifica_dei_nodi***
‘**rpc.mountd**’	`mountd:` ***specifica_dei_nodi***	`mountd:` ***specifica_dei_nodi***
‘**rpc.nfsd**’	`nfsd:` ***specifica_dei_nodi***	`nfsd:` ***specifica_dei_nodi***
‘**rpc.lockd**’	`lockd:` ***specifica_dei_nodi***	`lockd:` ***specifica_dei_nodi***
‘**rpc.statd**’	`statd:` ***specifica_dei_nodi***	`statd:` ***specifica_dei_nodi***
‘**rpc.rquotad**’	`rquotad:` ***specifica_dei_nodi***	`rquotad:` ***specifica_dei_nodi***

È molto probabile che molti di questi demoni siano insensibili al contenuto dei file ‘`/etc/hosts.allow`’ e ‘`/etc/hosts.deny`’; tuttavia, se nel proprio sistema si utilizzano questi file, è meglio scrivere una riga di più in questi file, anche se inutile, piuttosto che dimenticarsene e avere problemi in seguito. Pertanto, per abilitare l’accesso a tutti questi demoni, conviene utilizzare le direttive seguenti nel file ‘`/etc/hosts.allow`’:

```
portmap: specifica_dei_nodi
mountd: specifica_dei_nodi
nfsd: specifica_dei_nodi
lockd: specifica_dei_nodi
statd: specifica_dei_nodi
rquotad: specifica_dei_nodi
```

Per converso, può essere conveniente inserire le righe seguenti nel file ‘`/etc/hosts.deny`’, allo scopo di escludere gli accessi che non provengano dai nodi autorizzati espressamente:

```
portmap: ALL
mountd: ALL
nfsd: ALL
lockd: ALL
statd: ALL
rquotad: ALL
```

36.3.2 Verifica del servizio

«

Quando il servizio NFS è attivo, si può verificare il funzionamento e l'utilizzo di questo con il programma '**showmount**':

```
showmount [opzioni] [nodo]
```

Se non si indica un nodo, viene interrogato il servizio NFS presso l'elaboratore locale.

Tabella 36.27. Alcune opzioni.

Opzione	Descrizione
`-a` `--all`	Elenca i clienti che utilizzano il proprio servizio e anche le directory che questi hanno innestato.
`-e` `--exports`	Elenca le directory esportate dal servente locale o dal servente remoto (se indicato come ultimo argomento del comando).

Quando si interroga la situazione dell'utilizzo in corso, le informazioni vengono tratte dal file '`/var/lib/xtab`', che però potrebbe mostrare l'utilizzo attuale di directory che in realtà non lo sono più.

36.3.3 Porte coinvolte

Il servizio NFS si avvale per il suo funzionamento del Portmapper e di altri demoni specifici. In alcuni casi, questi demoni comunicano utilizzando porte TCP o UDP definite in modo dinamico, pubblicizzate poi dal Portmapper stesso. I punti di riferimento costanti sono solo quelli seguenti:

Porta TCP o UDP	Demone
111	Portmapper
2049	'**rpc.nfsd**'

36.3.4 Dal lato del cliente

Con i sistemi GNU/Linux, l'utilizzo di un file system di rete richiede solo che il kernel sia stato predisposto per questo. Non occorrono programmi demone, basta il normalissimo '**mount**'.

Per innestare un file system di rete si interviene in modo analogo a quello di una unità di memorizzazione locale, con la differenza fondamentale del modo di esprimere il dispositivo virtuale corrispondente al file system remoto da connettere.

nodo_remoto **:** ***directory_remota***

La notazione sopra riportata rappresenta la porzione di file system remoto cui si vuole accedere, attraverso l'indicazione simultanea dell'elaboratore e della directory di partenza.

Supponendo che l'elaboratore *dinkel.brot.dg* conceda l'utilizzo della directory '`/usr/`' e successive, l'elaboratore *roggen.brot.dg* potreb-

be sfruttarne l'occasione attraverso il programma '**mount**' nel modo seguente:

```
# mount -t nfs dinkel.brot.dg:/usr /usr[Invio]
```

Inoltre, nell'elaboratore *roggen.brot.dg* si potrebbe aggiungere una riga nel file '/etc/fstab' in modo da automatizzarne la connessione (19.4.1.6).

```
dinkel.brot.dg:/usr  /usr        nfs      defaults      0  0
```

Sia attraverso il programma '**mount**' (preceduti dall'opzione '**-o**'), sia nel file '/etc/fstab' (nel campo delle opzioni), possono essere specificate delle opzioni particolari riferite a questo tipo di file system. L'elenco seguente mostra solo alcune di queste opzioni, che possono avere rilevanza quando si innesta un file system di rete.

Opzione	Descrizione
rsize=***n***	Permette di specificare la dimensione dei pacchetti utilizzati in lettura da parte del cliente NFS. Il valore predefinito è di 1024 byte.
wsize=***n***	Permette di specificare la dimensione dei pacchetti utilizzati in scrittura da parte del cliente NFS. Il valore predefinito è di 1024 byte.

Opzione	Descrizione
`timeo=`***n***	Permette di definire il valore del *timeout*, espresso in decimi di secondo, per il completamento delle richieste. In pratica, se entro quel tempo non si ottiene una conferma, si verifica un *minor timeout* e l'operazione viene ritentata con una durata di *timeout* doppia. Quando si raggiunge un *timeout* massimo di 60 secondi si verifica un *major timeout*. Il valore predefinito è sette, corrispondente a 0,7 secondi.
`hard`	Stabilisce che la connessione deve essere ritentata all'infinito, anche dopo un *major timeout*. È la modalità di funzionamento predefinita.
`soft`	Stabilisce che venga generato un errore di I/O non appena si verifica un *major timeout*. Questa modalità si contrappone a quella '**`hard`**'.
`intr`	Permette l'interruzione di una chiamata NFS attraverso l'uso di segnali. Può essere utile per interrompere una connessione quando il servente non risponde.
`nosuid`	Evita di prendere in considerazione i permessi di tipo SUID e SGID dei file eseguibili.

In condizioni normali, conviene usare le opzioni '**`rw`**', '**`hard`**' e '**`intr`**', come nell'esempio seguente che rappresenta sempre una direttiva del file '`/etc/fstab`':

```
…
dinkel.brot.dg:/home   /home   nfs   rw,hard,intr    0   0
…
```

Per motivi di sicurezza, può essere utile anche l'opzione '**nosuid**', se si teme che un programma compromesso, presente nel file system remoto, possa acquisire privilegi particolare e intaccare l'elaboratore locale dal quale lo si avvia. Si vedano comunque le pagine di manuale *mount(8)* e *nfs(5)*.

36.4 NIS

«

Il NIS,[678] o *Network information service*, è un sistema di gestione di dati amministrativi concentrati in una sola fonte, rendendoli disponibili a tutta una rete in modo uniforme.

Il NIS è stato ideato e sviluppato originariamente dalla Sun Microsystems denominandolo originariamente *Yellow pages* (YP). Per questa ragione, molti programmi di servizio che riguardano la gestione del NIS hanno il prefisso '**yp**'; inoltre, a volte si parla di «servizi YP» invece di «servizi NIS».

Il NIS è un meccanismo che si sovrappone alla gestione amministrativa di un sistema Unix tipico, ma questo avviene in un modo non perfettamente integrato. Quando si introduce il NIS, si inserisce un livello di intermediazione tra l'utente e il sistema di amministratore preesistente.

36.4.1 Concentrazione amministrativa del NIS versione 2

Lo scopo del NIS è quello di concentrare in un solo elaboratore la gestione di una serie di file amministrativi. La tabella 36.32 elenca alcuni file di configurazione, tipici di un sistema Unix, che possono essere gestiti in questo modo.

Tabella 36.32. Elenco di alcuni dei file amministrativi gestibili comunemente attraverso il NIS.

File	Descrizione
‘`/etc/passwd`’	Informazioni sugli utenti.
‘`/etc/group`’	Gruppi di utenti.
‘`/etc/shadow`’	Parole d’ordine oscurate (quando gestibili).
‘`/etc/aliases`’	Alias di posta elettronica.
‘`/etc/hosts`’	Traduzione degli indirizzi IP dei nodi della rete locale.
‘`/etc/networks`’	Traduzione degli indirizzi IP delle sottoreti (locali).
‘`/etc/protocols`’	Nomi e numeri dei protocolli di rete.
‘`/etc/rpc`’	Numeri delle chiamate RPC.
‘`/etc/services`’	Abbinamento dei servizi di rete ai numeri di porta corrispondenti.

È bene chiarire subito che il supporto alle parole d’ordine oscurate non è disponibile in tutti i NIS esistenti; inoltre, il protocollo NIS (fino alla versione 2) rende difficile il loro utilizzo in modo «sicuro», nel senso di mantenere effettivamente nascoste le stringhe cifrate corrispondenti alle parole d’ordine di accesso degli utenti.

La concentrazione amministrativa si attua facendo in modo che le in-

formazioni dei file che interessano siano gestite a partire da un solo nodo. Generalmente, l'utilità del NIS sta nella possibilità di amministrare gli utenti da un'unica origine, facendo in modo che questi vengano riconosciuti in tutti gli elaboratori di un certo «dominio», senza dover essere inseriti effettivamente in ognuno di questi.

Gli esempi che si fanno nel capitolo sono volti principalmente al raggiungimento di questo risultato, concentrando così l'amministrazione dei file '`/etc/passwd`', '`/etc/group`' e '`/etc/shadow`'.

36.4.1.1 Mappe NIS

«

Il NIS non utilizza i file amministrativi così come sono, ne crea una copia; queste copie sono denominate «mappe». I file di mappa sono in formato DBM, dove si memorizzano solo coppie di dati: chiave-valore. Per questo motivo, a seconda della struttura dei file amministrativi originali, si possono generare più mappe differenti.

Quando si attiva il NIS, non si possono più utilizzare i vecchi comandi amministrativi (come '**`passwd`**', '**`chsh`**', ecc.), o quantomeno non conviene, perché il NIS non si accorge (autonomamente) dei cambiamenti apportati ai file tradizionali. Bisogna utilizzare i comandi specifici del NIS, in modo che i cambiamenti siano annotati immediatamente nelle mappe e poi siano propagati nei file amministrativi normali del servente NIS.

La tabella 36.33 riporta l'elenco di alcune delle mappe tipiche della gestione NIS. La collocazione di questi file dipende dal dominio NIS, descritto nella sezione seguente, e corrisponde in pratica a '`/var/yp/`***`dominio_nis`***`/`'.

Tabella 36.33. Elenco di alcune mappe NIS.

Mappa	Descrizione
‘`passwd.byname`’	Utenti per nome.
‘`passwd.byuid`’	Utenti per numero UID.
‘`group.byname`’	Gruppi per nome.
‘`group.bygid`’	Gruppi per numero GID.
‘`shadow.byname`’	Utenti per nome (dal file ‘`/etc/shadow`’).
‘`mail.aliases`’	Alias di posta elettronica.
‘`hosts.byname`’	Nodi per nome.
‘`hosts.byaddr`’	Nodi per indirizzo.
‘`networks.byname`’	Reti locali per nome.
‘`networks.byaddr`’	Reti locali per indirizzo.
‘`protocols.byname`’	Protocolli di rete per nome.
‘`protocols.bynumber`’	Protocolli di rete per numero.
‘`rpc.byname`’	Chiamate RPC per nome.
‘`rpc.bynumber`’	Chiamate RPC per numero.
‘`services.byname`’	Servizi di rete per nome.

36.4.1.2 Dominio NIS

Quando si attiva un servizio NIS in un nodo, in modo che questo renda disponibili le informazioni relative a un gruppo di elaboratori, si deve definire un dominio NIS corrispondente. Questo non ha niente a che fare con i domini utilizzati dal servizio DNS, ma generalmente, anche se potrebbe sovrapporsi perfettamente a un dominio di questo tipo, conviene utilizzare nomi distinti che non abbiano un nesso logico o intuitivo.

Più precisamente, è meglio dire che si stabilisce prima l’estensione del dominio NIS che si vuole creare, quindi si deve «eleggere» il nodo più adatto a fungere da servente NIS. Infatti, questo elaboratore

deve trovarsi in una posizione conveniente nella rete, in modo che sia accessibile facilmente da tutti gli elaboratori del dominio NIS. Oltre a questo è bene che si tratti di una macchina adeguata all'estensione del dominio: maggiore è il numero di clienti, maggiore è la frequenza con cui deve rispondere a richieste del protocollo NIS.

I file di mappa di un servente NIS sono raggruppati distintamente per dominio, nella directory '`/var/yp/`***dominio_nis***`/`'.

36.4.1.3 Servente principale e serventi secondari

«

Finora si è fatto riferimento a un servente NIS unico per tutto il suo dominio di competenza. Quando si attiva un servizio di questo tipo, tutti gli elaboratori clienti di questo dominio dipendono completamente dal servente per tutte quelle informazioni che sono state concentrate sotto la sua amministrazione. Se l'elaboratore che offre questo servizio dovesse venire a mancare per qualsiasi motivo, come un guasto, tutti i suoi clienti sarebbero in grave difficoltà.

Per risolvere il problema, si possono predisporre dei serventi NIS secondari, o *slave*, che riproducono le informazioni del servente principale, o *master*.

Il motivo per il quale si utilizza il servizio NIS è quello di uniformare e concentrare la gestione di informazioni di un gran numero di elaboratori, altrimenti non sarebbe giustificato l'impegno necessario alla sua attivazione. Di conseguenza, è praticamente obbligatorio attivare dei serventi secondari, sia per attenuare i rischi di blocco del sistema globale, sia per ridurre il carico di richieste NIS su un'unica macchina.

La presenza di serventi secondari impone la creazione di meccanismi automatici per il loro allineamento, generalmente attraverso il sistema Cron.

36.4.2 Distinzione dei ruoli tra servente e cliente

Finora è stato preso in considerazione il compito del servente NIS, senza valutare i clienti, ma all'inizio la distinzione dei compiti può sembrare confusa.

Il cliente NIS è un programma demone che si occupa di fornire al sistema in cui è in funzione le informazioni che altrimenti verrebbero ottenute dai soliti file di configurazione. La situazione tipica è quella della procedura di accesso: se il nome dell'utente non viene trovato nel file '`/etc/passwd`' locale, il cliente NIS cerca di ottenerlo dal servente NIS.

In pratica, le funzionalità di servente e cliente sono indipendenti: ci possono essere elaboratori che fungono da serventi, altri che utilizzano il programma cliente per accedere alle informazioni e altri ancora che fanno entrambe le cose.

Se si pensa che il servente NIS principale deve contenere tutte le informazioni che vengono condivise dai programmi clienti presso gli altri elaboratori, potrebbe sembrare inutile l'attivazione del programma cliente nello stesso servente. Tuttavia, le cose cambiano quando si considerano i serventi secondari. Questi non dispongono delle informazioni che ha l'elaboratore corrispondente al servente principale; per ottenerle occorre attivare il cliente NIS in modo che si possa mettere in comunicazione con il servente principale.

Nel sistema NIS così strutturato, i clienti cercano le informazioni, riferite al loro dominio, dal servente che risponde più rapidamente.

Ciò viene determinato generalmente attraverso una richiesta circolare (broadcast). Questo, tra le altre cose, è uno dei punti deboli del NIS: dal momento che qualunque elaboratore può rispondere a una chiamata circolare, chiunque è in grado di intromettersi per cercare di catturare delle informazioni.

36.4.2.1 Propagazione delle informazioni

«

Quando si deve intervenire per modificare qualche informazione di quelle che sono condivise attraverso il NIS, si presentano situazioni differenti a seconda delle circostanze. Queste si traducono in modalità diverse di propagazione delle modifiche nell'intero sistema NIS. Si distinguono due situazioni fondamentali:

- la modifica di un'informazione nell'elaboratore di origine (il servente principale) sui dati di partenza;
- la modifica di un'informazione attraverso gli strumenti offerti dal sistema NIS.

Nel primo caso le azioni da compiere sono:

1. aggiornare le mappe del servente principale;
2. aggiornare le mappe dei serventi secondari.

Nel secondo caso le azioni da compiere sono:

1. aggiornare i file di configurazione corrispondenti nel servente principale
2. aggiornare le mappe del servente principale
3. aggiornare le mappe dei serventi secondari

Quando si interviene manualmente sui file di configurazione di partenza del servente principale, per esempio quando si vuole aggiungere o eliminare un utente, si deve poi comandare manualmente l'aggiornamento delle mappe NIS; eventualmente si può pilotare anche l'aggiornamento dei serventi secondari, attraverso un cosiddetto *push*.

Quando si utilizzano gli strumenti offerti da NIS per modificare la configurazione dei dati condivisi, ciò può avvenire solo attraverso un cliente, il quale si occupa di contattare il servente principale che poi deve provvedere ad aggiornare i file normali e le mappe.

La propagazione delle mappe modificate ai serventi secondari potrebbe essere un problema. Per questo si utilizza generalmente il sistema Cron in ogni servente secondario, in modo da avviare periodicamente il comando necessario a metterli in comunicazione con il servente principale e verificare così la presenza di aggiornamenti eventuali.

Dalla precisione del funzionamento di questo sistema di propagazione derivano delle conseguenze pratiche che, a prima vista, possono sembrare assurde. Si può immaginare cosa può accadere quando un utente cambia la propria parola d'ordine da un cliente NIS. Questo contatta il servente principale che provvede ad aggiornare le mappe e il file '`/etc/passwd`'. Ma fino a che i serventi secondari non ricevono l'aggiornamento, i clienti che li utilizzano continuano a permettere l'accesso con la parola d'ordine vecchia. Questo può capitare allo stesso elaboratore dal quale è stata compiuta l'operazione di modifica, se questo utilizza il servizio di un servente secondario non aggiornato. In queste condizioni, l'utente che ha appena cambiato parola d'ordine e tenta un altro accesso sulla stessa macchina,

potrebbe trovarsi spaesato di fronte al rifiuto che gli si presenta.

36.4.3 NIS e DNS

Il NIS permette di distribuire le informazioni contenute nei file '`/etc/hosts`' e '`/etc/networks`', i quali consentono di risolvere i nomi dei nodi della rete locale, quando non si vuole fare uso di un DNS. Attraverso questa possibilità è poi possibile configurare il file '`/etc/host.conf`' dei vari clienti NIS, in modo che venga utilizzata tale informazione. Di solito si tratta di indicare una riga come quella seguente:

```
...
order hosts,nis
...
```

Tuttavia, nel momento stesso in cui si stabilisce di utilizzare il NIS, si decide di trattare l'organizzazione della rete locale seriamente, ma ciò comporta che anche la risoluzione dei nomi sia gestita in modo adeguato. Pertanto diventerebbe un controsenso la pretesa di gestire la risoluzione dei nomi solo attraverso il NIS, quando con poco impegno si può attivare un servente DNS. Al limite si possono unire le due cose:

```
...
order hosts,bind,nis
...
```

36.4.4 RPC

Il NIS utilizza le chiamate RPC per comunicare. Questo significa che è necessaria la presenza del Portmapper in funzione sia nei nodi serventi, sia nei nodi clienti (si veda eventualmente la sezione 36.2).

È anche importante verificare che i servizi di sincronizzazione, *time service*, siano previsti nel controllo del supervisore dei servizi di rete. Il file '`/etc/inetd.conf`' potrebbe contenere le righe seguenti:

```
# Time service is used for clock synchronization.
time            stream  tcp     nowait  root    internal
time            dgram   udp     wait    root    internal
```

Si osservi comunque che in alcune distribuzioni GNU, in base alla configurazione predefinita del supervisore dei servizi di rete, il servizio TIME attraverso il protocollo UDP non viene fornito, ma il servizio NIS dovrebbe funzionare ugualmente.

Se si devono apportare delle modifiche al file di configurazione del supervisore dei servizi di rete, bisogna poi ricordarsi di riavviarlo (sezione 36.1).

36.4.5 Allestimento di un servente NIS versioni 1 e 2

Gli elementi indispensabili di un servente NIS sono i programmi '**`ypserv`**' e '**`makedbm`**'. Il primo svolge il ruolo di demone in ascolto delle richieste NIS per il dominio di competenza, il secondo è necessario per convertire i file di configurazione normali in file DBM, cioè nelle mappe NIS.

Nel caso di un servente principale è anche opportuna la presenza di altri due demoni: '**`rpc.yppasswdd`**' e '**`rpc.ypxfrd`**'. Il primo serve a permettere la modifica delle parole d'ordine degli utenti attraverso il sistema NIS, il secondo serve a facilitare l'aggiornamento ai serventi secondari.

La configurazione di '**ypserv**' e '**rpc.ypxfrd**' può dipendere dal modo in cui sono stati compilati i sorgenti rispettivi. In generale si utilizza il file '`/etc/ypserv.conf`' per definire il comportamento di entrambi i programmi; inoltre '**ypserv**' può far uso di '`/etc/ypserv.securenets`' per conoscere gli indirizzi di rete da cui può accettare interrogazioni NIS, oppure può riutilizzare i tradizionali '`/etc/hosts.allow`' e '`/etc/hosts.deny`'. Per saperlo basta usare l'opzione '**-version**', come nell'esempio seguente:

```
# ypserv -version[Invio]

  ypserv - NYS YP Server version 1.1.7 (with tcp wrapper)
```

L'esempio mostra il risultato di un '**ypserv**' compilato in modo da avvalersi dei file '`/etc/hosts.allow`' e '`/etc/hosts.deny`', gli stessi che utilizza il TCP wrapper allo scopo di filtrare gli accessi ai programmi controllati dal supervisore dei servizi di rete.

```
  ypserv - NYS YP Server version 1.3.12 (with securenets)
```

Questo esempio ulteriore riguarda invece il risultato di un '**ypserv**' compilato in modo da avvalersi di '`/etc/ypserv.securenets`' (o di un file analogo collocato in una posizione diversa nel file system.

Prima di poter avviare il servente '**ypserv**', oltre a provvedere per la sua configurazione, occorre necessariamente che il Portmapper RPC sia in funzione e che il dominio NIS sia stato definito. In assenza di una sola di queste due condizioni, il programma '**ypserv**' non funziona, nel senso che non si riesce ad avviarlo.

36.4.5.1 Dominio NIS

Il dominio NIS viene definito attraverso '**domainname**', nel modo seguente:

```
domainname dominio_nis
```

Quando viene usato senza argomenti, si ottiene il nome del dominio NIS; in questo modo si può controllare se l'impostazione è corretta. Per esempio, l'impostazione del dominio NIS *rost.nis-yp* può essere fatta e controllata nel modo seguente:

```
# domainname rost.nis-yp [Invio]

# domainname [Invio]

  rost.nis-yp
```

Mentre l'impostazione del dominio è di competenza dell'utente '**root**', la verifica può essere fatta anche da un utente comune.

Di solito, si può fare riferimento a questo programma anche con altri nomi:

```
domainname [opzioni] [dominio_nis]
```

```
nisdomainname [opzioni] [dominio_nis]
```

```
ypdomainname [opzioni] [dominio_nis]
```

L'utilizzo tipico di '**domainname**' è riservato agli script della procedura di inizializzazione del sistema. Le istruzioni necessarie potrebbero essere organizzate nel modo seguente:

```
# Set the NIS domain name
if [ -n "$NISDOMAIN" ]
then
    domainname $NISDOMAIN
else
    domainname ""
fi
```

Oppure in modo alternativo anche come segue, dove il nome del dominio è contenuto in un file. In tal caso, bisogna fare attenzione al fatto che il file in questione deve essere composto esclusivamente da una riga, altrimenti viene presa in considerazione solo l'ultima, ma se questa è vuota, il dominio non viene definito.

```
# Set the NIS domain name
if [ -f "/etc/nisdomain" ]
then
    domainname -F /etc/nisdomain
else
    domainname ""
fi
```

36.4.5.2 Avvio del servente

«

In condizioni normali, '**ypserv**' non richiede l'uso di argomenti particolari, al massimo si tratta di controllare il file di configurazione '`/etc/ypserv.conf`' e l'eventuale '`/etc/ypserv.securenets`' (prima si deve verificare con l'opzione '**-v**' se questo file è necessario, o se al suo posto si usano i file di configurazione del TCP wrapper). In ogni caso, è importante che la directory '`/var/yp/`' sia sta-

ta creata (al suo interno si dovrebbe trovare un file-make, ma questo viene mostrato in seguito).

```
# ypserv[Invio]
```

Se tutto va bene, il programma si avvia sullo sfondo e si disassocia dalla shell, diventando un processo figlio di quello iniziale (Init).

```
# pstree[Invio]

  init-+-...
       |-portmap
       |-...
       `-ypserv
```

Se il Portmapper RPC non fosse attivo, oppure se non fosse stato definito il dominio NIS, l'avvio di '**ypserv**' non dovrebbe riuscire. Eventualmente, si può verificare il funzionamento del Portmapper stesso, attraverso il comando seguente:

```
# rpcinfo -p localhost[Invio]

    program vers proto   port
     100000    2   tcp    111  portmapper
     100000    2   udp    111  portmapper
```

Le righe che si vedono dall'esempio mostrato sono la dichiarazione esplicita del funzionamento del Portmapper. Per verificare espressamente la connessione con '**ypserv**', si può usare il comando seguente:

```
# rpcinfo -u localhost ypserv[Invio]

  program 100004 version 1 ready and waiting
  program 100004 version 2 ready and waiting
```

La sintassi per l'avvio di '**ypserv**' è molto semplice:

```
ypserv [opzioni]
```

L'elenco seguente descrive alcune opzioni della riga di comando di '**ypserv**' che possono essere utili.

Opzione	Descrizione
`-d` [*percorso_yp*] `--debug` [*percorso_yp*]	Utilizzando questa opzione si fa in modo che '**ypserv**' funzioni in modalità diagnostica. Per questo, invece di passare sullo sfondo, continua a funzionare occupando il terminale dal quale è stato avviato, emettendo informazioni particolareggiate su ciò che avviene attraverso lo standard error. Eventualmente si può indicare un percorso come argomento dell'opzione, intendendo fare in modo che '**ypserv**' utilizzi le mappe contenute a partire da quella directory, invece di quelle che si trovano a partire da '`/var/yp/`'.
`-b` `--dns`	Specifica che se un nodo non viene identificato diversamente, si deve utilizzare il servizio DNS.
`-v` `--version`	Visualizza i dati riferiti alla particolare versione di '**ypserv**'. Questa indicazione è molto importante, soprattutto per sapere quali file vengono utilizzati per controllare gli indirizzi che possono accedere al servizio.

Il programma '**ypserv**', quando tutto è configurato correttamente,

viene controllato dalla procedura di inizializzazione del sistema, attraverso uno dei suoi script. L'esempio che segue rappresenta un modo semplice per ottenere questo, dove la variabile di ambiente ***NISDOMAIN*** viene usata per contenere il dominio NIS; se manca questa variabile non ha senso avviare il servente NIS.

```
if [ -n "$NISDOMAIN" ]
then
    if [ -f /usr/sbin/ypserv ]
    then
        /usr/sbin/ypserv
        echo ypserv
    fi
fi
```

Quello mostrato è solo uno dei tanti modi; in generale bisogna ricordare che si può avviare il servizio NIS solo dopo aver avviato il Portmapper.

Nelle distribuzioni più accurate, è normale trovare uno script apposito che permette di avviare e di interrompere l'attività del servente NIS, assieme a tutto quello di cui potrebbe avere bisogno. Questo genere di script può trovarsi nelle directory '`/etc/rc.d/init.d/`', '`/etc/init.d/`' e altre possibili.

36.4.5.3 Configurazione principale

La configurazione di '`/etc/ypserv.conf`' riguarda il funzionamento di '**`ypserv`**' e '**`rpc.ypxfrd`**' in ogni caso. quando si fanno dei cambiamenti a questa configurazione occorre riavviare i demoni o inviare loro un segnale '**`SIGHUP`**'.

L'impostazione di questo file può essere anche molto complicata. In linea di massima ci si può fidare della configurazione predefinita, o

dei suggerimenti posti nei suoi commenti.

Il file può contenere commenti, rappresentati inizialmente dal simbolo '**#**', righe vuote o bianche, direttive riferite a opzioni e direttive riferite a regole di accesso. Le direttive di opzione hanno la forma seguente, dove la parola chiave '**yes**' attiva l'opzione, mentre '**no**' la disattiva.

opzione : [yes|no]

L'elenco seguente descrive tali opzioni.

Opzione	Descrizione
`dns : [yes|no]`	Attivando questa opzione, si fa in modo che il servente NIS utilizzi il DNS quando gli vengono richieste informazioni sui nodi che non può risolvere con le mappe '**hosts.***'. Il valore predefinito è '**no**' e questa opzione può essere attivata anche attraverso la riga di comando, '**--dns**', cosa che prevale su quanto stabilito nel file di configurazione.
`xfr_check_port : [yes|no]`	Attivando questa opzione, il servente principale deve utilizzare una porta inferiore al numero 1024. Il valore predefinito è '**yes**'.

Le direttive di accesso hanno invece il formato seguente:

nodo : ***mappa*** : ***livello_sicurezza*** : ***soppressione*** [: ***campo***]

- ***nodo***

  Si tratta di un indirizzo IP che può rappresentare un solo nodo o un gruppo. La rappresentazione può essere fatta attraverso un indirizzo IP incompleto, o la coppia indirizzo/maschera. Un indirizzo IP incompleto rappresenta tutti gli indirizzi che iniziano in quel modo, per cui, per esempio, «192.168.» equivale alla notazione 192.168.0.0/255.255.0.0, dove il secondo indirizzo è la maschera.

- ***mappa***

  Il nome della mappa, oppure un asterisco per identificare tutte le mappe.

- ***livello_sicurezza***

  Il livello, o il tipo di sicurezza, viene definito attraverso una parola chiave: '**`none`**', '**`port`**', '**`deny`**', '**`des`**'.

Parola chiave	Descrizione
`none`	Concede qualunque accesso.
`port`	Permette di accedere se la richiesta viene da una porta inferiore al numero 1024, ma solo se è stata specificata la soppressione.
`deny`	Vieta l'accesso alla mappa in questione.
`des`	Richiede l'autenticazione DES. Può funzionare solo se le librerie utilizzate sono in grado di gestire questa funzionalità.

- ***soppressione***

  Può contenere solo una tra le parole chiave '**yes**' e '**no**', dove '**yes**' attiva la soppressione del campo specificato. La soppressione implica che al suo posto viene collocata una «x», se il controllo della porta rivela che la richiesta proviene da un accesso non privilegiato.

- ***campo***

  Serve a specificare quale campo deve essere soppresso. Quello predefinito è il secondo.

L'esempio seguente rappresenta una configurazione predefinita di una distribuzione GNU:

```
# The following, when uncommented,  will give you shadow
# like passwords. Note that it will not work if you have
# slave NIS servers in your network that do not run the same
# server as you.

# Host        : Map                 : Security    : Passwd_mangle
#
# *           : passwd.byname       : port        : yes
# *           : passwd.byuid        : port        : yes
# *           : *                   : none

# This is the default - restrict access to the shadow
# password file, allow access to all others.
*             : shadow.byname       : port
*             : passwd.adjunct.byname : port
*             : *                   : none
```

36.4.5.4 Configurazione dei diritti di accesso

Il file ‘`/etc/ypserv.securenets`’ viene usato da ‘**`ypserv`**’ per sapere quali sono gli indirizzi ammessi a eseguire interrogazioni nel sistema NIS. Ma bisogna anche ricordare che ‘**`ypserv`**’ potrebbe essere stato compilato per non usare questo file, utilizzando al suo posto ‘`/etc/hosts.allow`’ e ‘`/etc/hosts.deny`’. Questo lo si determina utilizzando l’opzione ‘**`-v`**’.

Nel caso in cui ‘**`ypserv`**’ utilizzi il file ‘`/etc/ypserv.securenets`’, se questo manca o è vuoto, vengono consentiti tutti gli accessi in modo indiscriminato. Ogni volta che si modifica il file è necessario riavviare ‘**`ypserv`**’, oppure gli si deve inviare un segnale ‘**`SIGHUP`**’.

A parte i commenti (rappresentati dalle righe che iniziano con il simbolo ‘**`#`**’) e le righe vuote, questo file è fatto principalmente per annotare coppie di indirizzi IP, dove il primo è la maschera e il secondo l’indirizzo della rete a cui si vuole concedere l’accesso. L’esempio seguente è simile a quello che si trova nella pagina di manuale *ypserv(8)* e dovrebbe essere sufficiente a comprendere il meccanismo.

```
# Consente le connessioni dallo stesso elaboratore locale
# (è necessario). Equivale a 255.255.255.255 127.0.0.1
host 127.0.0.1

# Permette le connessioni da tutti gli elaboratori della
# rete locale 192.168.1.0
255.255.255.0   192.168.1.0
```

Anche se potrebbe essere inutile, se il proprio sistema utilizza i file ‘`/etc/hosts.allow`’ e ‘`/etc/hosts.deny`’, è bene occupar-

si della loro configurazione anche per ciò che potrebbe riguardare il NIS. Quelle che seguono sono le direttive che potrebbero essere inserite in '`/etc/hosts.allow`':

```
portmap: specifica_dei_nodi
ypserv: specifica_dei_nodi
ypbind: specifica_dei_nodi
yppasswd: specifica_dei_nodi
```

Per converso, può essere conveniente inserire le righe seguenti nel file '`/etc/hosts.deny`', allo scopo di escludere gli accessi che non provengano dai nodi autorizzati espressamente:

```
portmap: ALL
ypserv: ALL
ypbind: ALL
yppasswd: ALL
```

36.4.5.5 Configurazione e preparazione delle mappe

«

Le mappe NIS, come già accennato, sono collocate nella directory '`/var/yp/`***dominio_nis***`/`'. I file delle mappe esistenti, per il solo fatto di esserci, definiscono implicitamente quali sono i dati amministrativi che vengono gestiti in quel dominio NIS particolare. La loro creazione e il loro aggiornamento, avvengono attraverso un file-make che si trova nella directory '`/var/yp/`' e che generalmente viene utilizzato attraverso uno script. Il problema, semmai, sta nella necessità eventuale di modificare tale file-make per definire quali mappe debbano essere costruite.

In generale è indispensabile la lettura di questo file, per verificare come sono le impostazioni attuali. Si possono notare certamente molti commenti che spiegano il significato delle direttive che vengono date

(può trattarsi di assegnamenti a variabili che poi sono riutilizzate nel file-make stesso). È molto importante osservare bene la conformazione dell'obiettivo '**all**'; nell'esempio seguente, questo obiettivo richiede probabilmente la modifica manuale per includere le mappe che si intendono gestire, secondo l'esempio commentato che lo precede:

```
#all     ethers hosts networks protocols rpc services \
#        passwd group shadow passwd.adjunct netid netgrp \
#        publickey mail timezone locale netmasks

all:  passwd group shadow ypservers
```

L'esempio successivo mostra invece un obiettivo '**all**' controllato da una variabile, dove proprio le mappe per la gestione del file '`/etc/shadow`' sono controllate in modo automatico, in base alla presenza del file stesso:

```
# If you don't want some of these maps built, feel free to comment
# them out from this list.

ALL =   passwd group hosts rpc services netid protocols netgrp networks
#ALL += publickey mail ethers bootparams printcap
#ALL += amd.home auto.master auto.home auto.local
#ALL += timezone locale netmasks

# Autodetect /etc/shadow if it's there
ifneq ($(wildcard $(SHADOW)),)
ALL +=  shadow
endif

# Autodetect /etc/passwd.adjunct if it's there
ifneq ($(wildcard $(ADJUNCT)),)
ALL +=  passwd.adjunct
endif

all:    $(ALL)
```

In questo file-make esiste comunque un'altra cosa molto importante da controllare:

```
# If we have only one server, we don't have to push the maps
# to the slave servers (NOPUSH=true). If you have slave
# servers, change this to "NOPUSH=false" and put all
# hostnames of your slave servers in the file
# /var/yp/ypservers.
NOPUSH=true
```

Nella prima parte viene definito, attraverso una variabile, se il servente deve occuparsi di spedire gli aggiornamenti (*push*) ai serventi secondari. In questo caso, commentando l'assegnamento della variabile ***NOPUSH*** si ottiene di mantenere attivo questo aggiornamento.[9]

Una volta predisposto il file-make, si può usare il programma '**make**', senza argomenti, oppure si può utilizzare un comando specifico (è la scelta più elegante, mentre '**make**' è la scelta più semplice quando si raggiunge una certa dimestichezza con il sistema).

```
# /usr/lib/yp/ypinit -m[Invio]
```

Il vero vantaggio nell'utilizzo di questo programma (che poi è in realtà uno script), sta nel fatto che provvede a costruire al volo il file '`/var/yp/servers`', con l'elenco dei serventi competenti per il dominio che si sta predisponendo.

```
At this point, we have to construct a list of the hosts
which will run NIS servers.  dinkel.brot.dg is in the list
of NIS server hosts. Please continue to add the names for
the other hosts, one per line.
When you are done with the list, type a <control D>.
        next host to add:  dinkel.brot.dg
        next host to add:
```

Questa operazione va condotta dall'elaboratore che deve svolgere il ruolo di servente principale, di conseguenza, il suo indirizzo deve apparire per primo. Supponendo di avere un secondo elaboratore da utilizzare come servente secondario, si può aggiungere il suo nome e quindi terminare con la combinazione [*Ctrl d*].

```
next host to add: roggen.brot.dg[Invio]

next host to add: [Ctrl d]

  The current list of NIS servers looks like this:

  dinkel.brot.dg
  roggen.brot.dg

Is this correct? [y/n: y][Invio]

  We need some  minutes to build the databases...
  Building /var/yp/rost.nis-yp/ypservers...
  Running /var/yp/Makefile...
  NIS Map update started on Thu Jul 25 12:00:00 CEST 2002
  make[1]: Entering directory `/var/yp/rost.nis-yp'
  Updating passwd.byname...
  Updating passwd.byuid...
  Updating group.byname...
  Updating group.bygid...
  Updating shadow.byname...
  make[1]: Leaving directory `/var/yp/rost.nis-yp'
  NIS Map update completed.
```

Questo è il tipo di risultato che si può osservare quando tutto procede regolarmente. Se non si utilizza lo script '**ypinit**', si salta la predisposizione del file '`/var/yp/rost.nis-yp/ypservers`', che però potrebbe essere già stato ottenuto da un'esecuzione precedente di

'**ypinit**'. In pratica, lo script '**ypinit**' va utilizzato convenientemente la prima volta che si allestisce il servente, mentre le altre volte è sufficiente utilizzare solo '**make**' dalla directory '`/var/yp/`':

```
# cd /var/yp [Invio]

# make [Invio]
```

36.4.5.6 Gestione delle parole d'ordine

Perché gli utenti del servizio NIS possano modificare la propria parola d'ordine di accesso, è necessario che nel servente principale sia in funzione il demone '**rpc.yppasswdd**':

```
rpc.yppasswdd [opzioni]
```

Le opzioni disponibili dipendono molto dalla versione di questo programma e dal modo con cui è stato compilato. È da questo programma che dipende anche la possibilità o meno di utilizzare '**ypchsh**' e '**ypchfn**'. In generale, utilizzandolo senza opzioni particolari, è possibile solo la modifica delle parole d'ordine.

Va però osservato che se nel servente NIS si esegue il comando

```
# cd /var/yp ; make [Invio]
```

questi cambiamenti si perdono, perché si ripristinano i dati provenienti dai file di sistema '`/etc/passwd`' e '`/etc/shadow`'. Pertanto, il problema del cambiamento della parola d'ordine andrebbe risolto con strumenti differenti, tali da assicurare l'aggiornamento dei file di sistema tradizionali presso il servente NIS.

36.4.6 Predisposizione del servente secondario

I serventi secondari, ammesso che se ne vogliano avere, devono poter comunicare con il servente principale, ma naturalmente ciò richiede implicitamente che questi, oltre che serventi secondari, siano anche dei clienti. Più avanti viene spiegato come predisporre un cliente NIS; per il momento è bene affrontare ugualmente il problema, per mantenere mentalmente il collegamento con quanto già trattato sul servente principale.

Un servente secondario richiede le stesse cose del servente principale, a eccezione del demone '**`rpc.yppasswdd`**' che nel servente secondario non ha ragione di esistere. Questo significa che:

- si deve impostare il dominio NIS;
- si deve configurare '**`ypserv`**' attraverso '`/etc/ypserv.conf`' e '`/etc/ypserv.securenets`', oppure gli altri file del TCP wrapper.

Si è già accennato al fatto che il servente secondario deve avere il cliente NIS in funzione, ma la differenza più interessante sta nell'assenza del file-make nella directory '`/var/yp/`'. Naturalmente, il file-make può anche esserci, ma non deve essere preso in considerazione.

36.4.6.1 Riproduzione delle mappe nel servente secondario

Anche il servente secondario, per poter compiere il suo lavoro, deve disporre delle mappe NIS. Queste vengono create, copiandole dal servente principale, attraverso il comando seguente:

```
/usr/lib/yp/ypinit -s servente_nis_principale
```

In pratica, si avvia '**ypinit**' con l'opzione '**-s**', indicando il nome dell'elaboratore che ospita il servente principale. Per esempio, se il servente principale è *dinkel.brot.dg*, il comando corretto è il seguente:

```
# /usr/lib/yp/ypinit -s dinkel.brot.dg [Invio]
```

Perché l'operazione funzioni correttamente, occorre che il cliente NIS sottostante sia configurato e funzionante. In pratica, prima di utilizzare '**ypinit**', si può verificare che sia tutto in ordine con il comando seguente:

```
# ypwhich -m [Invio]
```

Questo deve restituire il nome del servente principale.

36.4.6.2 Sincronizzazione

La presenza di serventi secondari introduce nel sistema NIS dei problemi di sincronizzazione di questi con il servente principale. Oltre a tutto, lo stesso procedimento di sincronizzazione accresce i problemi di sicurezza, dal momento che periodicamente viaggiano informazioni delicate nella rete.

Ci sono tre modi per sincronizzare i serventi secondari, ma non tutti funzionano sempre, a causa degli accorgimenti utilizzati per ridurre i problemi di sicurezza.

1. Quando il servente principale viene aggiornato, dovrebbe essere in grado di inviare ai serventi secondari le modifiche alle mappe

(*push*). Questa operazione non funziona se i serventi secondari non sono in ascolto in quel momento, inoltre non funziona anche in altre circostanze, sempre per motivi di sicurezza.

2. I serventi secondari possono comunicare periodicamente con il servente principale per verificare la presenza di aggiornamenti delle mappe. Questa operazione richiede nel servente principale la presenza in funzione del demone '**`rpc.ypxfrd`**'.

3. In ultima analisi, i serventi secondari si aggiornano con il comando '**`ypinit -s`** ***servente_principale***'.

Per quanto riguarda il secondo punto, il NIS offre generalmente tre script predisposti opportunamente per eseguire i compiti di aggiornamento. Si tratta di: '**`ypxfr_1perhour`**', '**`ypxfr_1perday`**' e '**`ypxfr_2perday`**'. Questi si trovano nella directory '`/usr/lib/yp/`' e sono pensati per essere inclusi in un file crontab, come nell'esempio seguente che rappresenta precisamente il file '`/etc/crontab`'.

```
20 *    * * * root /usr/lib/yp/ypxfr_1perhour
40 6    * * * root /usr/lib/yp/ypxfr_1perday
55 6,18 * * * root /usr/lib/yp/ypxfr_2perday
```

I diversi script si occupano di trasferire mappe differenti. In particolare, quello eseguito ogni ora è predisposto per trasferire le informazioni sugli utenti (la cosa più urgente).

Dal momento che non si può fare affidamento sul sistema di aggiornamento pilotato dal servente principale (quello del primo punto), se per qualche motivo l'aggiornamento a mezzo di '**`ypxfr`**' non funziona, occorre ripiegare necessariamente sull'uso periodi-

co di '**ypinit -s**', eventualmente collocando anch'esso in un file crontab.

Come già accennato, il demone '**rpc.ypxfrd**' viene utilizzato solo nel servente principale per facilitare l'aggiornamento delle mappe nei serventi secondari. La sua presenza non è indispensabile, ma è utile per accelerare il processo di aggiornamento.

```
rpc.ypxfrd [opzioni]
```

Generalmente può essere utilizzato senza argomenti e dovrebbe essere gestito direttamente dalla procedura di inizializzazione del sistema.

36.4.7 Organizzazione di una distribuzione

«

Quando la propria distribuzione GNU è ben organizzata, non è necessario intervenire direttamente nel file '`/var/yp/Makefile`'; inoltre, è normale che siano già predisposti correttamente gli script per il controllo del NIS attraverso la procedura di inizializzazione del sistema.

Nel caso particolare delle distribuzioni Debian, lo script della procedura di inizializzazione del sistema che controlla il NIS è '`/etc/init.d/nis`'. Questo script, a sua volta, utilizza le indicazioni contenute nel file '`/etc/default/nis`' per sapere se deve essere attivato un servizio NIS come servente principale, secondario, o come cliente. Nell'esempio seguente si intende allestire un servente principale, in cui i file contenenti le parole d'ordine si trovano nella directory '`/etc/`' (come avviene di solito), che consente la modifica remota della shell:

```
# /etc/default/nis     Configuration settings for the NIS
#                      daemons.

# Are we a NIS server and if so what kind
# (values: false, slave, master)
NISSERVER=master

# Location of the master NIS password file (for yppasswdd).
# If you change this make sure it matches with
# /var/yp/Makefile.
YPPWDDIR=/etc

# Do we allow the user to use ypchsh and/or ypchfn ? The
# YPCHANGEOK fields are passed with -e to yppasswdd, see
# it's manpage. Possible values: "chsh", "chfn", "chsh,chfn"
YPCHANGEOK=chsh
```

36.4.8 Cliente NIS

Gli elaboratori che devono condividere le informazioni amministrate con il NIS, devono utilizzare il demone '**ypbind**', configurato opportunamente. In tal modo, su tali elaboratori, invece di utilizzare le informazioni amministrative locali, vengono usate quelle concentrate dal NIS.

La configurazione di '**ypbind**' avviene attraverso i file '`/etc/yp.conf`' e '`/etc/nsswitch.conf`'. Il primo serve a definire come raggiungere i serventi; il secondo definisce l'ordine di utilizzo dei servizi (*Name service switch*).

Come nel caso dei serventi, anche i clienti richiedono la definizione del dominio NIS, attraverso '**domainname**'. Se il dominio non viene predisposto '**ypbind**' non può funzionare.

Anche il cliente richiede la presenza della directory ‘`/var/yp/`’. Al suo interno viene creata la directory ‘`binding/`’.

Anche il cliente richiede l’attivazione del Portmapper RPC.

36.4.8.1 Gli utenti

A seconda delle caratteristiche particolari del cliente, sono possibili delle configurazioni speciali per ciò che riguarda l’accesso da parte degli utenti. Quando la loro gestione è compito del NIS, si può configurare il cliente in modo da definire una graduatoria nella ricerca dei dati che identificano l’utente al momento dell’accesso. Di solito si cerca prima l’utente nel file ‘`/etc/passwd`’ locale, quindi si prova con il NIS.

A parte questo particolare abbastanza semplice, si può porre il problema di voler concedere l’accesso su un certo elaboratore solo ad alcuni utenti definiti attraverso il NIS, oppure, più semplicemente, si può volere escludere l’accesso da parte di qualcuno. Per ottenere questo occorre intervenire sul file ‘`/etc/passwd`’ utilizzando record con notazioni particolari; cosa che qui non viene descritta.

In generale, per fare in modo che gli utenti NIS del dominio a cui si fa riferimento possano accedere da un certo cliente, occorre aggiungere in coda un record speciale nei file ‘`/etc/passwd`’, ‘`/etc/group`’ e ‘`/etc/shadow`’:

- ‘`/etc/passwd`’

```
+::::::
```

- ‘`/etc/group`’

```
+:::
```

- ‘/etc/shadow’

```
+::::::
```

Questo record viene interpretato come il punto in cui si vogliono inserire virtualmente gli utenti NIS.

36.4.8.2 Attivazione del demone

‘**ypbind**’ è il demone necessario all’attivazione dell’accesso alle informazioni fornite da un servente NIS; è in pratica il cliente NIS. Utilizza la directory ‘/var/yp/binding/’ per collocarci all’interno un file contenente le informazioni sul dominio NIS per il quale è stato avviato.

```
ypbind [opzioni]
```

‘**ypbind**’ utilizza la configurazione del file ‘/etc/yp.conf’ per trovare i serventi e quella del file ‘/etc/nsswitch.conf’ per stabilire l’ordine di utilizzo delle informazioni amministrative.

In caso di difficoltà, può essere avviato con l’opzione ‘**-debug**’, in modo da farlo funzionare in primo piano, per controllare le informazioni diagnostiche emesse attraverso lo standard error.

La configurazione principale di questo demone avviene per mezzo del file ‘/etc/yp.conf’, il quale serve a definire come accedere ai serventi.

‘**ypbind**’ potrebbe essere in grado di utilizzare solo l’ultima riga di questo file. Di conseguenza, è bene limitarsi a una sola direttiva.

Il file può contenere tre tipi di direttive, descritte dai modelli sintattici seguenti:

```
domain dominio_nis server nodo
```

```
domain dominio_nis broadcast
```

```
ypserv nodo
```

La prima definisce che per il dominio NIS indicato si deve interpellare il servente specificato; la seconda definisce che per il dominio si devono usare delle chiamate circolari a tutta la rete (locale); l'ultima definisce semplicemente un servente, indipendentemente dal dominio.

Quando si utilizza il sistema della chiamata circolare (broadcast), si rischia di ricevere la risposta da un possibile servente fasullo, collocato appositamente per sostituirsi a quelli veri allo scopo di carpire informazioni dai clienti. Se non si temono attacchi di questo tipo, la chiamata circolare è il modo migliore che consente al cliente di scegliersi il servente (quello che risponde prima).

Il servente può essere indicato per nome o per numero IP. Nel primo caso, è necessario che il sistema sia in grado di risolvere il nome in modo indipendente dal NIS (evidentemente). In generale, è conveniente utilizzare l'indirizzo IP per questo scopo.

L'esempio seguente mostra l'unica riga di un file '`/etc/yp.conf`' in cui si stabilisce che per il dominio *rost.nis-yp* si deve usare la

chiamata circolare.

```
domain rost.nis-yp broadcast
```

Il file '`/etc/nsswitch.conf`' viene usato dalla libreria C per attuare il NSS, ovvero il *Name service switch*, che in pratica stabilisce l'ordine in cui devono essere cercate le informazioni (se attraverso il NIS, file locali o altro). Pertanto, il modo corretto di configurare questo file dipende strettamente dal tipo e dalla versione della libreria utilizzata. Si veda a questo proposito quanto descritto nella pagina di manuale *nsswitch.conf(5)*, oppure nell'ipertesto Info: *info libc*.

Quello che segue è la configurazione proposta in una distribuzione GNU particolare.

```
# /etc/nsswitch.conf
#
# Example configuration of GNU Name Service Switch
# functionality. If you have the 'glibc-doc' and 'info'
# packages installed, try: 'info libc "Name Service Switch"'
# for information about this file.

passwd:         compat
group:          compat
shadow:         compat

hosts:          files dns
networks:       files

protocols:      db files
services:       db files
ethers:         db files
rpc:            db files
```

```
netgroup:       nis
```

36.4.8.3 Altri programmi di contorno

Dal lato del cliente sono importanti altri programmi di contorno. Si tratta precisamente di '**ypwhich**', '**ypcat**', '**ypmatch**' e '**yppasswd**'.

Il programma '**ypwhich**' permette di conoscere quale sia il servente NIS utilizzato dal cliente oppure quale sia precisamente il servente principale per una certa mappa.

```
ypwhich [opzioni]
```

Opzione	Descrizione
	Senza opzioni, il programma '**ypwhich**' mostra il servente NIS usato.
`-d` ***dominio***	Utilizza un dominio differente da quello predefinito. Per usare questa opzione occorre comunque che tale dominio diverso sia stato collegato.
`-m` [***mappa***]	Permette di conoscere quale sia il servente principale per la particolare mappa specificata, o per tutte quelle che vengono raggiunte.

Seguono alcuni esempi di utilizzo di '**ypwhich**'.

```
$ ypwhich [Invio]
```

Emette il nome dell'elaboratore che funge da servente NIS per quel particolare cliente.

```
$ ypwhich -m [Invio]
```

Emette l'elenco delle mappe gestire dal NIS con i rispettivi serventi principali competenti.

Il programma '**ypcat**' emette il contenuto di una mappa indicata come argomento della riga di comando. Questo programma dipende da '**ypbind**'.

```
ypcat [opzioni] mappa
```

Opzione	Descrizione
`-d` ***dominio***	Utilizza un dominio differente da quello predefinito. Per usare questa opzione occorre comunque che tale dominio diverso sia stato collegato.

L'esempio seguente serve a emettere il contenuto della mappa corrispondente all'elenco dei gruppi per nome.

```
$ ypcat group.byname [Invio]
```

Il programma '**ypmatch**' emette il valori corrispondenti a una o più chiavi di una mappa. Questo programma dipende da '**ypbind**'.

```
ypmatch [opzioni] chiave... mappa
```

Opzione	Descrizione
`-d` ***dominio***	Utilizza un dominio differente da quello predefinito. Per usare questa opzione occorre comunque che tale dominio diverso sia stato collegato.

Seguono alcuni esempi di utilizzo di '**ypmatch**'.

```
$ ypmatch tizio caio passwd.byname [Invio]
```

Emette i record corrispondenti agli utenti '**tizio**' e '**caio**'.

```
$ ypmatch 500 passwd.byuid [Invio]
```

Emette il record corrispondente all'utente identificato dal numero UID 500.

I nomi '**yppasswd**', '**ypchsh**' e '**ypchfn**' sono tre alias dello stesso programma. A seconda di quale viene usato per avviarlo, si intende cambiare la parola d'ordine, la shell o le informazioni personali.

```
yppasswd [utente]
```

```
ypchsh [utente]
```

```
ypchfn [utente]
```

Questi comandi si sostituiscono ai soliti '**passwd**', '**chsh**' e '**chfn**', i quali hanno effetto solo localmente, quando si vuole intervenire sulle utenze gestite dal NIS. A questo proposito, è bene considerare la possibiltà di fare «sparire» i comandi normali, in modo da non creare confusione agli utenti, predisponendo dei collegamenti simbolici opportuni per fare in modo che '**passwd**', '**chsh**' e '**chfn**' avviino rispettivamente i corrispondenti '**yppasswd**', '**ypchsh**' e '**ypchfn**'.

Questi comandi, quando vengono invocati, si mettono in contatto

con il servente principale, nel quale deve essere in funzione il demone '**rpc.passwdd**'. È da questo demone che dipende la possibilità di cambiare tali valori, ma potrebbe capitare che sia abilitata solo la sostituzione delle parole d'ordine.

Solo l'utente '**root**' può indicare il nome di un altro utente attraverso la riga di comando.

36.4.9 Directory personali

Quando si gestiscono gli utenti (e i gruppi) attraverso il NIS, si intende permettere a tutti questi utenti di utilizzare indifferentemente tutte le macchine su cui si fa funzionare il cliente NIS. Per raggiungere questo obiettivo, occorre fare in modo che le rispettive directory personali (*home*) siano accessibili da qualunque postazione. Evidentemente è necessario usare uno spazio condiviso in rete, attraverso il protocollo NFS.

Il modo più semplice potrebbe essere quello di predisporre una partizione apposita in un servente NFS, innestando tale file system nella directory '`/home/`' di ogni cliente NIS. Come si può intuire non si tratta di una soluzione ottimale, comunque è qualcosa di pratico, almeno inizialmente.

Il file system condiviso deve essere accessibile in lettura e scrittura.

La gestione del protocollo NFS è descritta nella sezione 36.3.

36.4.10 Porte coinvolte

Il servizio NIS si avvale per il suo funzionamento del Portmapper e di altri demoni specifici, come descritto nel capitolo. In generale, questi demoni comunicano utilizzando porte TCP o UDP definite in

modo dinamico, pubblicizzate poi dal Portmapper stesso. Pertanto, a parte il Portmapper che opera alla porta 111, non esiste la possibilità di controllare il traffico NIS per mezzo di filtri di pacchetto che usano come riferimento le porte TCP e UDP.

Eventualmente, molti dei demoni del servizio NIS possono accettare un opzione della riga di comando con la quale si specifica espressamente un numero di porta; in questo modo si può stabilire una convenzione interna e sfruttare questa per la configurazione di un firewall.

36.5 DHCP

«

La sigla DHCP sta per *Dynamic host configuration protocol* e identifica un protocollo per la configurazione automatica dei nodi di rete.[10] Il problema riguarda evidentemente le reti locali in cui si desidera centralizzare il problema della configurazione dei nodi di rete in un servente, senza intervenire in ogni nodo, singolarmente.

La configurazione dei clienti, definita nel servente DHCP, può essere statica o dinamica; quando questa è dinamica, il servente DHCP concorda con i clienti che lo contattano un tempo di validità per la configurazione assegnata, sulla base del fatto che i clienti siano comunque riconoscibili dal servente attraverso l'indirizzo Ethernet. Ciò permette all'elaboratore cliente che riceve una configurazione dinamica di mantenere quella configurazione per un certo tempo, senza che questa debba essere necessariamente ridefinita a ogni riavvio. Questo tempo di validità viene indicato con il termine *lease* ed è compito del servente tenere memoria delle configurazioni già assegnate; d'altro canto i clienti devono comunque richiedere ogni volta al servente i dati per la propria configurazione.

Il termine inglese *lease* fa intendere che il cliente «affitta» la sua posizione nella rete.

36.5.1 Sistemazioni generali per il kernel Linux

Il cliente che tenta di contattare un servente DHCP deve utilizzare una chiamata circolare. Per questo, nel caso di un sistema GNU/Linux, i kernel utilizzati negli elaboratori clienti e quello del servente, devono essere stati predisposti opportunamente per il *multicasting* (sezione 8.3.7). Si verifica facilmente che sia disponibile questa caratteristica attraverso '**ifconfig**', dando una configurazione transitoria a un'interfaccia e quindi visualizzando il suo stato come nel caso seguente:

```
# ifconfig eth0 [Invio]

eth0      Link encap:Ethernet  HWaddr 00:A0:24:77:49:97
          inet addr:192.168.1.1  Bcast:192.168.1.255  Mask:255.255.255.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0
          TX packets:87 errors:0 dropped:0 overruns:0
          Interrupt:12 Base address:0xff80
```

In questo caso si vede apparire la parola '**MULTICAST**' che rappresenta l'attivazione della modalità corrispondente, risolvendo ogni dubbio.

Il servente DHCP deve essere in grado di trasmettere dei pacchetti all'indirizzo IP 255.255.255.255, corrispondente idealmente a «tutti i nodi». In circostanze eccezionali,[11] può darsi che per poterlo fare si debba creare un instradamento apposito, su **tutte** le interfacce di rete attraverso cui il servente deve essere raggiungibile e da cui deve poter rispondere.

```
# route add -host 255.255.255.255 dev eth0 [Invio]

# route add -host 255.255.255.255 dev eth1 [Invio]
```

L'esempio, in particolare, mostra l'instradamento attraverso le interfacce '**eth0**' e '**eth1**'.

In ultima analisi, un kernel Linux deve essere stato predisposto per la gestione di *Packet socket* e *Network packet filtering*. Nel file di configurazione della compilazione del kernel, queste voci corrispondono a '**CONFIG_PACKET**' e a '**CONFIG_NETFILTER**'. Si veda eventualmente il capitolo 8.3.7.

36.5.2 Rete di competenza e router

«

Teoricamente, dovrebbe essere possibile fare in modo che il servente DHCP riceva le richieste dei clienti anche se queste devono attraversare dei router. In pratica, ciò richiede che i router siano in grado di trasferire tali richieste, oppure che presso di loro sia presente un servizio intermedio di relè (*relay*). Comunque, si tratterebbe di una politica amministrativa discutibile. Infatti, in generale, il servente DHCP dovrebbe essere collocato nella rete fisica che si trova a servire, mentre le richieste dei clienti non dovrebbero poter attraversare i router.

L'utilizzo del protocollo DHCP può costituire un problema serio di sicurezza; in questo senso, sarebbe meglio se i router non fossero in grado di trasferire le connessioni con questo protocollo.

36.5.3 Conflitto con il supervisore dei servizi di rete

Normalmente, il protocollo DHCP utilizza la porta 67 UDP, che di solito è denominata '**bootps**'. Il supervisore dei servizi di rete potrebbe essere stato predisposto per la gestione del servizio BOOTP su quella porta. Per esempio, nel file '`/etc/inetd.conf`' che riguarda precisamente la configurazione di Inetd, potrebbe essere presente una riga simile a quella seguente, commentata nello stesso modo:

```
...
#bootps dgram   udp   wait   root   /usr/sbin/tcpd  bootpd
...
```

Se invece la gestione del servizio BOOTP fosse abilitata, ciò andrebbe in conflitto con i demoni usati per il DHCP, sia nel nodo del servente, sia nei nodi clienti.

36.5.3.1 Informazioni gestibili attraverso DHCP

Attraverso il protocollo DHCP, i nodi clienti possono ricevere una serie di informazioni utili a definire la propria collocazione nella rete circostante. Il minimo indispensabile di tali informazioni è costituito normalmente dall'indirizzo IPv4 e dalla maschera di rete relativa. Dipende poi dalle caratteristiche del servente la possibilità di offrire informazioni aggiuntive. L'elenco seguente è solo un esempio delle informazioni che potrebbero essere offerte:

- l'indirizzo IPv4 e la maschera di rete;
- l'indirizzo broadcast;
- il nome del nodo e il dominio relativo;

- l'indirizzo del router predefinito;
- l'indirizzo del servente DNS;
- l'indirizzo del servente di stampa;
- il dominio NIS;
- il servente NIS;
- il servente per la sincronizzazione dell'orologio.

36.5.4 Servente DHCP ISC

«

Il servente DHCP che si trova di solito nelle distribuzioni GNU è quello la cui produzione è stata finanziata da Internet Systems Consortium.[12] Viene fatta questa precisazione, perché negli stessi sistemi GNU potrebbe essere utilizzato un cliente di origine differente.

Il servente DHCP di ISC si compone del demone '**dhcpd**', il quale si avvale della configurazione contenuta nel file '`dhcpd.conf`' ('`/etc/dhcp*/dhcpd.conf`' o simile), inoltre utilizza il file '`dhcpd.leases`' (che potrebbe essere collocato nella directory '`/var/lib/dhcp*/`') per annotare gli indirizzi concessi ai vari clienti, finché questi restano validi. Questo ultimo file, '`dhcpd.leases`', deve esistere (vuoto) prima che il demone possa essere avviato la prima volta. Eventualmente, il demone '**dhcpd**' è in grado di offrire anche un servizio BOOTP, se la configurazione contiene le informazioni necessarie per la gestione di questo tipo di protocollo.

Il problema di organizzazione del servente si limita quindi alla configurazione del file '`dhcpd.conf`'.

Segue il modello sintattico per l'avvio del demone:

```
dhcpd [opzioni] [interfaccia...]
```

In generale, '**dhcpd**' non richiede alcun argomento nella riga di comando, limitandosi così a leggere la configurazione e a porsi in ascolto di tutte le interfacce in grado di gestire il multicast, funzionando come demone. L'indicazione di una o più interfacce di rete, alla fine degli argomenti, permette di specificare dove '**dhcpd**' deve porre la sua attenzione, ignorando le altre che fossero eventualmente presenti.

Opzione	Descrizione
`-p` ***n_porta***	Il demone '**dhcpd**' è in ascolto normalmente della porta UDP numero 67 (BOOTPS), ma ciò può essere cambiato attraverso questa opzione.
`-cf` ***file_di_configurazione***	Permette di definire un file di configurazione alternativo a quello predefinito.
`-lf` ***file_lease***	Permette di definire un file alternativo a quello predefinito per l'accumulo delle informazioni sui nodi che hanno ottenuto un indirizzo IP.

La configurazione con il file '`dhcpd.conf`' permette di definire il funzionamento di '**dhcpd**', sia per la gestione del protocollo DHCP, sia per BOOTP. Tuttavia, qui si intendono mostrare solo le direttive utili per il protocollo DHCP. In questo file sono ammessi i commenti, preceduti dal simbolo '**#**' e terminati dalla fine della riga in cui appaiono. È consentito inoltre spaziare le direttive attraverso righe vuote o righe bianche.

Le direttive sono organizzare in forma di struttura, in cui appare la

dichiarazione di ciò a cui fa riferimento tale struttura, seguita dall'indicazione di una serie di parametri specifici, racchiusi tra parentesi graffe:

```
[parametro_globale ; ]
[parametro_globale ; ]
...
dichiarazione {
        [parametro_specifico ; ]
        ...
        [sotto_dichiarazione {
                [parametro_più_specifico ; ]
                ...
        } ]
        ...
}
...
```

Lo schema sintattico è un po' confuso a prima vista, ma significa che il file può iniziare con una serie di direttive (facoltative) contenenti l'indicazione di alcuni parametri (viene chiarito in seguito di cosa può trattarsi), il cui effetto ha valore globale, salvo la possibilità di essere offuscati da definizioni contrastanti all'interno di direttive di dichiarazione.

Il file deve contenere almeno una direttiva di dichiarazione che può limitarsi a contenere dei parametri specifici, oppure può inglobare delle sotto-dichiarazioni.

La cosa migliore, per cominciare, è introdurre un esempio. Si sup-

ponga di volere servire la rete locale 192.168.1.0/255.255.255.0, specificando che gli indirizzi da 192.168.1.100 a 192.168.1.199 possono essere gestiti per le attribuzioni dinamiche di indirizzi IPv4. Il file di configurazione può limitarsi a contenere quanto segue:

```
subnet 192.168.1.0 netmask 255.255.255.0 {
    range 192.168.1.100 192.168.1.199;
}
```

La direttiva di dichiarazione '**subnet**', come si può intuire, è quella più importante per la gestione del DHCP. Nella maggior parte dei casi, la configurazione si compone di una o più direttive di questo tipo, contenenti probabilmente più parametri di quanto visto nell'esempio.

Prima di mostrare più in dettaglio le altre direttive, viene presentato un altro esempio che potrebbe soddisfare le esigenze più comuni di chi utilizza '**dhcpd**' (a parte i valori particolari che sono stati indicati). Rispetto all'esempio precedente si nota la presenza di due intervalli di indirizzi IPv4 da utilizzare per l'attribuzione automatica; per il resto, momentaneamente, dovrebbe essere intuitivo il significato.

```
subnet 192.168.1.0 netmask 255.255.255.0 {
    range 192.168.1.100 192.168.1.149;
    range 192.168.1.200 192.168.1.249;
    default-lease-time 604800;  # una settimana
    max-lease-time 2592000;     # 30 giorni
    option subnet-mask 255.255.255.0;
    option broadcast-address 192.168.1.255;
    option routers 192.168.1.1;
    option domain-name-servers 192.168.1.1, 192.168.1.2;
    option domain-name "brot.dg";
}
```

Prima di proseguire con la descrizione di alcuni tra dichiarazioni

e parametri, si osservi che i parametri sono terminati dal punto e virgola. È ammesso indicare più parametri sulla stessa riga, anche se in generale è preferibile evitarlo.

Dichiarazione	Descrizione

shared-network ***nome*** {
[***parametro*** ;]
...
dichiarazione {
...
}
...
}
	Come si osserva dalla sintassi, una dichiarazione '**shared-network**' è fatta per l'inclusione di altre dichiarazioni e non solo di parametri. Permette di specificare una rete condivisa, nel senso di due o più reti logiche che si trovano sulla stessa rete fisica. In questa situazione, è normale che la direttiva includa l'indicazione di più dichiarazioni '**subnet**', una per ogni rete logica. Il problema, semmai, è che quando si collocano dei nodi nuovi nella rete condivisa, non è possibile distinguere a quale delle reti logiche dovrebbero appartenere; di conseguenza, ottengono semplicemente il primo indirizzo libero nell'insieme globale.

Dichiarazione	Descrizione

`group {`
`  [`*parametro* `;` `]`
`  ...`
`  `*dichiarazione* `{`
`  ...`
`  }`
`  ...`
`}`
	La dichiarazione '**`group`**' serve solo a definire un raggruppamento di dichiarazioni, a cui attribuire una serie di parametri in modo predefinito. Evidentemente si tratta dei parametri che precedono le direttive delle dichiarazioni annidate.

`subnet` *indirizzo_di_rete* ↩
↪ `netmask` *maschera_di_rete* `{`
`  [`*parametro* `;` `]`
`  ...`
`}`
	La dichiarazione '**`subnet`**' serve a contenere l'indicazione di parametri specifici per la sottorete. Permette di definire una sottorete, indicata attraverso l'indirizzo e la maschera di rete.

Parametro	Descrizione

`authoritative;`
 	
`not authoritative;`
	L'opzione '**`authoritative`**' (opposta a '**`not authoritative`**' che invece è predefinita), consente di specificare che il servente è «autorevole» e che può riconfigurare i nodi che risultano configurati in modo errato.

Parametro	Descrizione
`default-lease-time` ***n_secondi*** `;`	Definisce il tempo predefinito per la scadenza dell'associazione tra nodo e indirizzo IP assegnato. Viene utilizzato se il cliente non richiede una durata differente.
`max-lease-time` ***n_secondi*** `;`	Definisce il tempo massimo per la scadenza dell'associazione tra nodo e indirizzo IP assegnato. Il cliente non può ottenere un tempo maggiore (che comunque può essere rinnovato).
`range` ***indirizzo_ip_iniziale indirizzo_ip_finale*** `;`	Indica l'intervallo di indirizzi IP utilizzabili in modo dinamico. Più intervalli separati possono essere indicati utilizzando più volte questo tipo di parametro.
`option subnet-mask` ***maschera_di_rete*** `;`	Permette di specificare la maschera di rete, modificando eventualmente quanto stabilito in modo predefinito.
`option broadcast-address` ↩ ↪***indirizzo_broadcast*** `;`	Permette di definire l'indirizzo broadcast.

Parametro	Descrizione
`option routers` ***indirizzo_ip_del_router*** `;`	Permette di indicare l'indirizzo IP del router predefinito.
`option domain-name-servers` ***indirizzo_dns*** `[,…];`	Permette di indicare un elenco di indirizzi di serventi DNS. Gli indirizzi sono separati attraverso una virgola.
`option domain-name "`***dominio***`";`	Stabilisce il nome a dominio. Di solito si tratta del dominio della rete o della sottorete a cui si fa riferimento.
`option nis-domain` ***dominio_nis*** `;`	Stabilisce il dominio NIS.
`option nis-servers` ***servente_nis*** `[,` ***servente_nis*** `]…;`	Indica uno o più serventi NIS.
`option lpr-servers` ***servente_lpr*** `[,` ***servente_lpr*** `]…;`	Indica uno o più serventi di stampa (stampanti di rete).
`option log-servers` ***servente_log*** `[,` ***servente_log*** `]…;`	Indica uno o più nodi in grado di ricevere annotazioni da aggiungere al registro del sistema.
`option root-path "`***nodo***`:/`***percorso***`";`	Indica il nodo e il percorso a partire dal quale è possibile innestare il file system.

Per conoscere tutte le «opzioni» che si possono inserire nel-

le direttive '**option**', si deve leggere la pagina di manuale *dhcp-options(5)*.

36.5.4.1 Avvio e arresto del servizio

In condizioni normali, il demone '**dhcpd**' viene controllato dalla procedura di inizializzazione del sistema, attraverso uno dei suoi script. L'esempio che segue rappresenta un modo semplice per ottenere questo, dove la variabile di ambiente ***INTERFACES*** viene usata per contenere l'elenco delle interfacce di rete da configurare:

```
#!/bin/sh
#
test -f /usr/sbin/dhcpd || exit 0
#
INTERFACES="eth0"
#
case "$1" in
  start)
        printf "Avvio del servizio DHCP: "
        /usr/sbin/dhcpd -q $INTERFACES
        echo
        ;;
  stop)
        printf "Disattivazione del servizio DHCP: "
        killall dhcpd
        echo
        ;;
  *)
        echo "Utilizzo: dhcp-server {start|stop}"
        exit 1
esac
```

Nel caso particolare della distribuzione GNU/Linux Debian, questo

script è certamente più complesso, ma fa uso proprio della variabile di ambiente ***INTERFACES*** che viene definita nel file '`/etc/default/dhcp3-server`':

```
# Defaults for dhcp initscript
# sourced by /etc/init.d/dhcp
# installed at /etc/default/dhcp3-server by the maintainer
# scripts

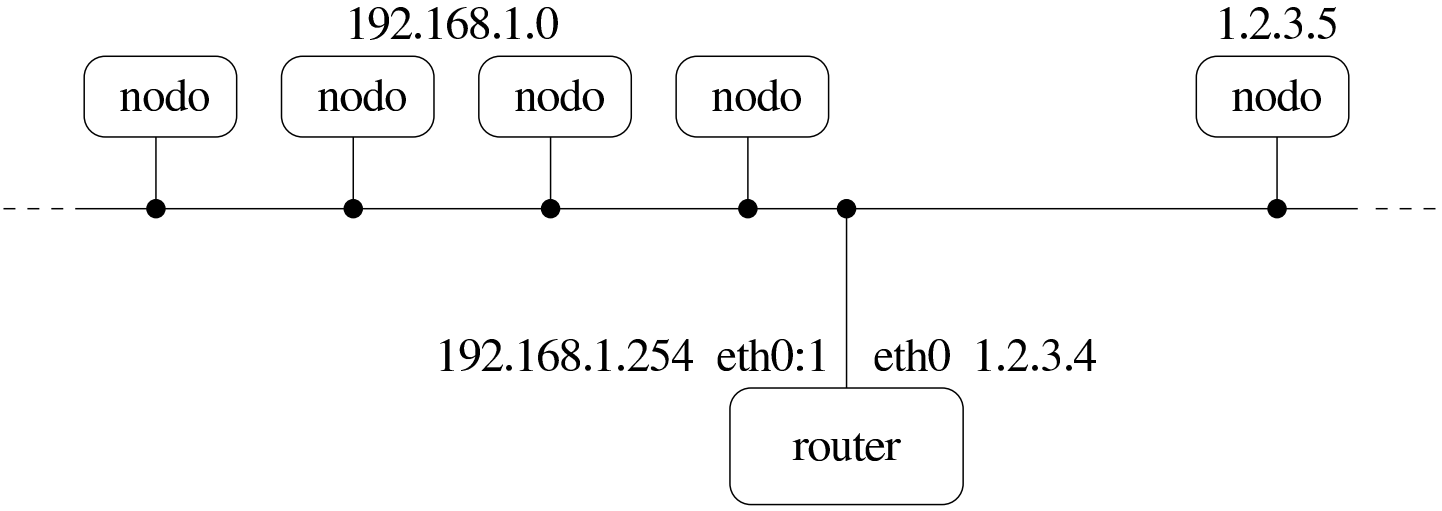
#
# This is a POSIX shell fragment
#

# On what interfaces should the DHCP server (dhcpd) serve
# DHCP requests?
# Separate multiple interfaces with spaces,
# e.g. "eth0 eth1".
INTERFACES="eth0"
```

36.5.4.2 Interfaccia di rete e alias con i sistemi GNU/Linux

Quando si utilizza il servente DHCP di ISC su un sistema GNU/Linux, occorre tenere presente che l'interfaccia di rete indicata alla fine della riga di comando di '**dhcpd**', deve essere reale; in pratica, non può trattarsi di un «alias», come potrebbe esserlo un nome del tipo '**eth0:1**'.

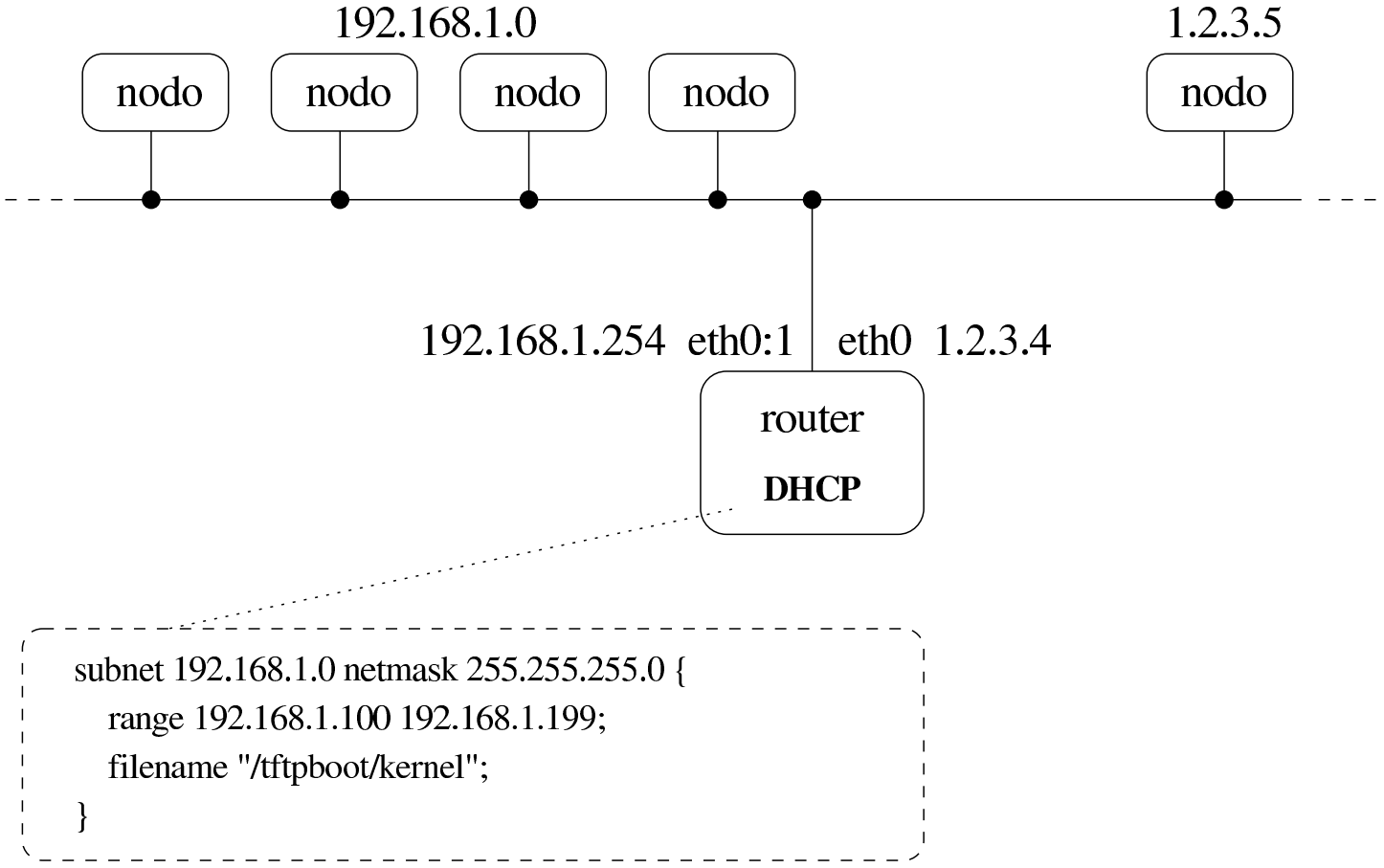
Figura 36.78. Un router per due reti che in realtà sono fisicamente la stessa.



Quando si configura un router con una sola interfaccia di rete reale (utilizzando il sistema GNU/Linux), diventa praticamente indispensabile fare riferimento al nome di interfaccia reale per ciò che si può considerare come la «rete esterna». Questa necessità dipende dal fatto che il programma '**`iptables`**', usato, per esempio, per configurare il NAT e un sistema di filtri, richiede l'indicazione di un nome di interfaccia reale, ma dovendo scegliere, in questo caso, è importante che il nome reale sia riferito alla rete esterna.

Se si vuole attivare un servizio DHCP all'interno di un elaboratore che è collegato a due reti (reali o virtuali), è ragionevole supporre che questo servizio serva per quella rete che si considera, in qualche modo, interna. Se però si sta lavorando nelle condizioni ipotizzate, dove si dispone di una sola interfaccia reale e si attribuiscono degli alias, dovendo utilizzare il nome reale dell'interfaccia per la rete esterna, finisce che il servizio DHCP opera proprio dove non serve.

Figura 36.79. In questo caso, il servizio DHCP interviene in un gruppo di indirizzi della rete 192.168.1.*, ma si trova formalmente a essere fornito dall'indirizzo 1.2.3.4. In questo caso, succede in particolare che il file '`/tftpboot/kernel`' risulta trovarsi presso l'elaboratore 1.2.3.4, mentre un sistema senza disco fisso (*diskless*) della rete 192.168.1.* si trova in difficoltà a raggiungerlo.



Purtroppo, non c'è modo di istruire il demone '**`dhcpd`**' di rispondere utilizzando l'indirizzo mittente che si preferisce per la rete interna. Il programma '**`dhclient`**' che viene descritto in una sezione apposita, può superare il problema, purché ci sia un router che consente di raggiungere l'indirizzo del lato esterno (si suppone che sia lo stesso nodo che ha questa interfaccia singola che esegue il compito di router); tuttavia, altri programmi non ne sono in grado; in particolare

l'avvio di un sistema senza disco potrebbe essere in crisi.

Eventualmente si può sfruttare un raggiro molto semplice: si configura temporaneamente l'interfaccia reale con l'indirizzo da usare per la rete interna; si avvia il demone '**dhcpd**'; si riconfigura l'interfaccia con l'indirizzo esterno e si dichiara un alias per l'indirizzo interno. In questo modo, il demone '**dhcpd**' continua a lavorare considerando l'indirizzo interno corretto:

```
# ifconfig eth0 192.168.1.254 [Invio]

# /usr/sbin/dhcpd -q eth0 [Invio]

# ifconfig eth0 1.2.3.4 [Invio]

# ifconfig eth0:1 192.168.1.254 [Invio]

...
```

Ovviamente, la sequenza mostrata delle operazioni è semplificata, in quanto non verifica la necessità eventuale di dover terminare il funzionamento di un demone '**dhcpd**' già attivo, inoltre non si considera la possibilità di disattivare l'interfaccia di rete prima di riconfigurarla.

36.5.5 Relè DHCP ISC

«

Nello stesso pacchetto del servente DHCP descritto nelle sezioni precedenti, si trova normalmente il demone '**dhcrelay**'. Questo è in grado di fungere da ripetitore per una richiesta fatta da un cliente DHCP, quando questa, diversamente, non può attraversare un router.

All'inizio del capitolo si è accennato al fatto che sarebbe meglio evitare che un servizio DHCP possa superare i router; tuttavia, chi

desidera utilizzare ugualmente tale possibilità, lo può fare attraverso questo programma.

```
dhcrelay [opzioni] servente_dhcp...
```

Il programma '**dhcrelay**' è un demone in grado di ritrasmettere le richieste fatte da un cliente DHCP a un servente che altrimenti non sarebbe raggiungibile. Nello stesso modo, le risposte vengono rinviate all'origine.

Il programma '**dhcrelay**' non richiede configurazione; l'unica cosa indispensabile è l'indicazione di almeno un servente DHCP alla fine della riga di comando.

Tabella 36.80. Alcune opzioni.

Opzione	Descrizione
`-p` ***n_porta***	Permette di specificare un numero di porta differente da quella standard (67).
`-i` ***interfaccia***	Permette di indicare in modo esplicito un'interfaccia di rete da cui '**dhcrelay**' può aspettarsi delle richieste da parte di clienti DHCP. Per indicare più interfacce, occorre usare più volte questa opzione. Questa opzione è utile in particolare per escludere eventualmente un'interfaccia di una rete fisica su cui potrebbe esserci già il servente DHCP relativo, in grado di intervenire da solo.

36.5.6 Cliente DHCP

«

Il cliente DHCP ha il compito di interpellare un servente attraverso una chiamata circolare fatta nella rete fisica in cui si trova lo stesso cliente, ottenendo da questo l'indicazione dell'indirizzo IPv4 da utilizzare, assieme ad altre informazioni di contorno eventuali. Successivamente, ha il compito di ripresentarsi presso il servente periodicamente, per evitare che scada il tempo concesso per l'identificazione che gli è stata attribuita (*lease*).

Il problema maggiore, semmai, è fare in modo che il sistema presso cui è in funzione il cliente DHCP sia in grado di adeguarsi alle informazioni ottenute in questo modo. Non basta sapere quale indirizzo IPv4 si può utilizzare per una certa interfaccia di rete, occorre anche configurarla e definire l'instradamento. A questo proposito, il cliente DHCP è un punto delicato, per cui la scelta, ammesso che ce ne sia più di una, va fatta pensando all'integrazione con il proprio sistema operativo.

36.5.6.1 Cliente DHCP ISC

«

Nel pacchetto DHCP di Internet Systems Consortium è disponibile il programma cliente '**dhclient**' per l'interrogazione di tale servizio:

```
dhclient [opzioni] [interfaccia...]
```

Il programma '**dhclient**', una volta terminata la prima fase di scansione, avvia uno script con il quale configura l'interfaccia di rete e l'instradamento, quindi si mette a funzionare sullo sfondo, come demone.

Tabella 36.81. Alcune opzioni.

Opzione	Descrizione
`-p` ***n_porta***	Permette di specificare un numero di porta differente da quella standard (68).
`-r`	Richiede espressamente di abbandonare l'indirizzo IPv4 ottenuto (*current lease*); con questa opzione, il programma termina di funzionare (non rimane in funzione come demone).
`-1`	Esegue una sola serie di tentativi; se non riesce a contattare un servente DHCP termina di funzionare.
`-q`	Fa in modo di non mostrare informazioni nel momento dell'avvio, prima di passare al funzionamento sullo sfondo.
`-cf` ***file_di_configurazione***	Permette di definire un file di configurazione alternativo a quello predefinito.
`-lf` ***file_lease***	Permette di definire un file alternativo a quello predefinito per l'accumulo delle informazioni ottenute (*lease*).
`-sf` ***file_script***	Permette di definire uno script alternativo a quello predefinito, per la riconfigurazione in base ai dati ottenuti.

Una volta avviato, quando ottiene le informazioni che servono da un servente DHCP, le accumula nel file '`dhclient.leases`' che dovrebbe trovarsi nella directory '`/var/lib/dhcp*/`', o nel file specificato con l'opzione '**`-lf`**'. Il contenuto di questo file potrebbe essere simile all'esempio seguente:

```
lease {
  interface "eth0";
  fixed-address 192.168.1.250;
```

```
  option subnet-mask 255.255.255.0;
  option routers 192.168.1.254;
  option dhcp-lease-time 86400;
  option dhcp-option-overload 3;
  option dhcp-message-type 5;
  option domain-name-servers 192.168.1.254;
  option dhcp-server-identifier 192.168.1.254;
  option broadcast-address 255.255.255.255;
  renew 1 2004/7/5 20:39:26;
  rebind 2 2004/7/6 07:57:59;
  expire 2 2004/7/6 10:57:59;
}
```

Il programma dovrebbe essere in grado di configurare automaticamente l'interfaccia di rete, l'instradamento locale e quello predefinito. Eventualmente può avere dei problemi a intervenire nel file '`/etc/resolv.conf`', per indicare il servente DNS; in tal caso è necessario costruire un proprio script che estragga questa informazione dal file '`dhclient.leases`'.

Il programma '**`dhclient`**' prevede anche l'uso di un file di configurazione, '`dhclient.conf`', che normalmente si colloca nella directory '`/etc/dhcp*/`', oppure può essere ridefinito con l'opzione '**`-cf`**'. Le cose più importanti da inserire in questo file sono le richieste da fare al servente DHCP, come si vede nell'esempio seguente che potrebbe essere usato per la maggior parte delle situazioni di utilizzo di tale programma:

```
request subnet-mask,
        broadcast-address,
        time-offset,
        routers,
        domain-name,
```

```
        domain-name-servers,
        host-name,
        netbios-name-servers,
        netbios-scope,
        time-servers,
        ntp-servers,
        root-path,
        nis-domain,
        nis-servers,
        lpr-servers,
        log-servers;
```

Per conoscere le altre direttive che, eventualmente, possono essere utilizzate per la configurazione, si deve consultare la pagina di manuale *dhclient.conf(5)*; inoltre, per conoscere tutte le «opzioni» del protocollo, si deve leggere la pagina di manuale *dhcp-options(5)*.

36.5.6.2 Script per l'utilizzo delle informazioni ottenute da un cliente DHCP ISC

Le informazioni che si possono ottenere attraverso un servizio DHCP sono molte e non è semplice standardizzarne l'utilizzo nell'ambito della procedura di inizializzazione del sistema. Pertanto, si può essere costretti a realizzare un proprio script per estrapolare i dati contenuti nel file '`/var/lib/dhcp*/dhclient.leases`'. Il file *allegati/net/dhcp-auto-configuration.txt* rappresenta la parte saliente di uno script del genere, da inserire in qualche modo nella procedura di avvio del sistema. L'esempio ha il solo scopo di mostrare come si può fare in pratica a gestire tali informazioni.

36.6 Informazioni sugli utenti della rete

I servizi di informazione sugli utenti della rete possono essere distinti in tre tipi, a seconda che si basino sul servizio di uno dei demoni seguenti:

- '**rwhod**'
- '**rpc.rusersd**'
- '**fingerd**'

L'attivazione dei servizi che forniscono informazioni sugli utenti sono fonte di problemi di sicurezza. In generale, sarebbero molto utili nelle reti locali chiuse; tuttavia, dal momento che le reti locali sono sempre più difficili da mantenere «chiuse», tali servizi diventano pericolosi in generale.

36.6.1 Who remoto

Si tratta di un sistema che raccoglie le informazioni sugli utenti connessi nella rete locale.[13] Le informazioni sono aggiornate frequentemente da un demone locale che, attraverso l'invio e la ricezione di messaggi broadcast, informa e ottiene informazioni dagli altri sistemi dove si trova in funzione lo stesso demone. Così, ogni elaboratore che ha in funzione questo demone ha una directory '`/var/spool/rwho/`' contenente una serie di file, uno per ogni elaboratore incontrato nella rete locale. Questi file rappresentano il risultato finale del sistema di raccolta di informazioni e ognuno di questi contiene l'indicazione degli utenti che utilizzano gli elaboratori della rete locale.

Il demone che si occupa di fornire e ricevere le informazioni sugli utenti connessi sui vari elaboratori della rete locale è '**rwhod**'. Dal momento che la comunicazione tra il demone locale e quelli degli altri elaboratori avviene attraverso messaggi broadcast, la rete deve essere in grado di gestire tali messaggi e il sistema di collezione delle informazioni risulta limitato all'ambito dell'indirizzo broadcast utilizzato. Il modello sintattico mostra che in generale non si usano argomenti per l'avvio di '**rwhod**':

```
rwhod
```

Il programma '**rwhod**' può essere avviato solo come demone autonomo, senza il controllo del supervisore dei servizi di rete; pertanto, per attivarlo in modo sistematico occorre predisporre uno script gestito dalla procedura di inizializzazione del sistema.

All'interno di ogni elaboratore che partecipa al servizio di condivisione delle informazioni sugli utenti, il programma '**rwho**' è quello che legge i file contenuti in '`/var/spool/rwho/`' per informare sugli utenti connessi agli elaboratori della rete locale:

```
rwho [-a]
```

Opzione	Descrizione
`-a`	Permette di non visualizzare le informazioni sugli utenti che da molto tempo risultano non avere alcuna interazione con il proprio sistema.

36.6.2 Informazioni attraverso RPC

«

È possibile richiedere informazioni attraverso le RPC. Per ottenerle, occorre che l'elaboratore dal quale si vogliono ricevere abbia in funzione il servizio RPC '**rusersd**', normalmente reso disponibile dal demone '**rpc.rusersd**'.[14] Naturalmente, trattandosi di un servizio RPC, occorre che anche il Portmapper sia stato attivato preventivamente (sezione 36.2).

Normalmente, il demone '**rpc.rusersd**' va avviato in maniera indipendente dal supervisore dei servizi di rete, attraverso la procedura di inizializzazione del sistema:

```
rpc.rusersd
```

Il programma '**rusers**', dal lato cliente, elenca gli utenti connessi agli elaboratori della rete locale, svolgendo in pratica il compito del programma '**users**', ma attraverso la rete. Per ottenere queste informazioni, utilizza una chiamata RPC e quindi instaura un collegamento con il demone '**rpc.rusersd**' presso gli elaboratori che rispondono:

```
rusers [-a] [-l] [nodo...]
```

Opzione	Significato mnemonico	Descrizione
`-a`	*all*	Mostra le informazioni di tutti i nodi che rispondono, anche se nessun utente vi accede in quel momento.

Opzione	Significato mnemonico	Descrizione
`-l`	*login*	Mostra informazioni dettagliate sugli accessi.

36.6.3 Finger: informazioni personali

Quando si parla di Finger[15] si fa riferimento alle informazioni personali contenute nel quinto campo del file '`/etc/passwd`', cioè al nominativo completo dell'utente. A volte, in questo campo si trovano informazioni addizionali, come l'ufficio, il numero telefonico dell'ufficio e il numero di casa. Sotto questo aspetto, tali informazioni sono molto delicate, pertanto questo tipo di servizio va attivato solo se strettamente necessario.[16]

Volendo, si possono rendere pubbliche queste informazioni, assieme ad altre che si raccolgono all'interno di file di configurazione contenuti nelle directory personali degli utenti, attraverso il demone '**`in.fingerd`**' (o solo '**`fingerd`**'), controllato dal supervisore dei servizi di rete.

```
in.fingerd [opzioni]
```

Nell'esempio seguente, viene mostrata la riga di '`/etc/inetd.conf`' in cui si dichiara il suo possibile utilizzo per quanto riguarda il caso particolare di Inetd:

```
…
finger  stream  tcp  nowait  root  /usr/sbin/tcpd in.fingerd
…
```

Segue la descrizione di alcune opzioni della riga di comando del demone '**in.fingerd**'.

Opzione	Significato mnemonico	Descrizione
`-w`	*welcome*	Con questa opzione, gli utenti remoti del servizio ricevono un benvenuto addizionale, contenente informazioni particolareggiate sul sistema in funzione. Dal momento che queste indicazioni possono essere utili a un ipotetico aggressore, generalmente si evita di utilizzare tale opzione.
`-u`	*user*	L'opzione '**-u**' permette di non accogliere richieste remote generalizzate. In pratica, si impedisce l'uso di un comando del tipo '**finger @*nodo***', in cui non appare esplicitamente il nome di un utente particolare.
`-l`	*log*	Attiva l'annotazione delle richieste nel registro di sistema.

In generale, per motivi di sicurezza è meglio avviare il demone con l'opzione '**-u**', in modo da evitare le richieste generalizzate a tutti gli utenti del sistema.

Il programma '**finger**' consente di visualizzare le informazioni utili a identificare gli utenti indicati come argomento. Gli utenti possono essere specificati anche utilizzando il simbolo '`@`' seguito dal nome dell'elaboratore. Se non vengono indicati nomi di utente, viene visualizzato l'elenco degli utenti connessi. Se si specifica il nome di

un elaboratore preceduto dal simbolo '`@`', viene visualizzato l'elenco degli utenti connessi a quell'elaboratore:

`finger` [***opzioni***] [***utente***…] [[***utente***]`@`***nodo***…]

Opzione	Significato mnemonico	Descrizione
`-s`	*status*	Visualizza il nominativo degli utenti, il nome reale, i terminali a cui sono connessi (con l'aggiunta di un asterisco nel caso sia impedita la scrittura, cosa che impedisce di inviare dei messaggi con il programma '**`write`**'), il tempo di inattività (questo non esclude che su quel terminale possa essere in uso un qualche programma interattivo), il momento in cui è avvenuto l'accesso e le informazioni addizionali sull'ufficio.

Opzione	Significato mnemonico	Descrizione
`-l`	*multi-line*	Fornisce tutte le informazioni che si potrebbero ottenere attraverso l'opzione '**`-s`**', assieme a tutte le altre disponibili: la directory personale, il telefono privato, la shell iniziale, la situazione della posta elettronica, assieme al contenuto dei file '`~/.plan`', '`~/.project`' e '`~/.forward`' (che si trovano nella directory personale di quell'utente). Questa è l'azione predefinita che corrisponde in pratica a fornire tutte le notizie disponibili sull'utente.

Segue la descrizione di alcuni esempi.

- `$` **`finger`**[*Invio*]

  Fornisce l'elenco degli utenti connessi al sistema locale.

- `$` **`finger @dinkel.brot.dg`**[*Invio*]

  Se l'elaboratore *dinkel.brot.dg* lo consente, fornisce l'elenco degli utenti connessi a quel sistema remoto. In caso contrario (quando il servente '**`in.fingerd`**' è stato avviato con l'opzione '**`-u`**') si dovrebbe ottenere un messaggio simile a quello seguente:

  ```
  Please supply a username
  ```

- `$` **`finger -l @dinkel.brot.dg`**[*Invio*]

Se l'elaboratore *dinkel.brot.dg* lo consente, fornisce tutte le informazioni disponibili sugli utenti connessi a quel sistema remoto.

- `$` **`finger -l tizio@dinkel.brot.dg`**[*Invio*]

  Se l'elaboratore *dinkel.brot.dg* lo consente, fornisce tutte le informazioni disponibili sull'utente '**`tizio`**', indipendentemente dal fatto che questo sia connesso o meno.

36.6.3.1 File personali

Quando il programma '**`finger`**' può funzionare, assieme alle informazioni personali dell'utente che può ottenere dal file '`/etc/passwd`', può emettere anche il contenuto di alcuni file predisposti dall'utente stesso: '`~/.plan`', '`~/.project`' e '`~/.forward`'.

Il file '`~/.forward`' serve a indicare un indirizzo di posta elettronica a cui viene dirottata la posta in modo automatico. Non riguarda quindi direttamente '**`finger`**', ma è una di quelle informazioni che questo servizio fornisce opportunamente, anche se in modo indiscreto. Gli altri due file possono essere usati da ogni utente per indicare informazioni addizionali. Generalmente si utilizza solo il primo, '`~/.plan`', per lo scopo di pubblicizzare notizie attraverso il servizio Finger. Segue l'esempio di quello che si potrebbe ottenere interrogando le notizie disponibili di un certo utente:

```
Login: daniele                          Name: daniele giacomini
Directory: /home/daniele                Shell: /bin/bash
Office Phone: 123456
On since Thu Mar 26 07:49 (MET DST) on tty1  10 minutes 3
seconds idle
     (messages off)
On since Thu Mar 26 09:37 (MET DST) on ttyp5 from :0.0
Mail forwarded to appunti2@gmail.com
No mail.
Project:
a2
No Plan.
```

36.7 Accesso remoto

Un gruppo di programmi storici consente di eseguire delle operazioni su elaboratori remoti, attraverso un protocollo di comunicazione **superato**, ma del quale è necessario conoscerne l'esistenza, per evitare di consentire accessi indesiderabili attraverso una configurazione predefinita non adeguata. I nomi di questi programmi iniziano convenzionalmente con una lettera «r» in modo da distinguerli da programmi equivalenti che svolgono la loro funzione in ambito locale.

Naturalmente, perché si possano essere eseguite delle operazioni remote, queste devono essere concesse attraverso demoni in grado di attuare quanto richiesto.[17]

Al posto dei protocolli LOGIN e SHELL, a cui si riferiscono i programmi descritti in questa sezione, vanno preferiti invece TELNET o SSH (sezioni 36.8 e 44.7).

L'esecuzione di un'elaborazione remota richiede il riconoscimento dell'utente, in modo da potere stabilire l'ambito e i privilegi in cui si deve trovare presso l'elaboratore remoto. Il riconoscimento può avvenire attraverso una sorta di procedura di accesso, durante il funzionamento del programma dal lato cliente, oppure può essere basato sulla semplice fiducia, concedendo l'accesso attraverso la preparazione di alcuni file di configurazione. Indubbiamente, la fiducia è un metodo molto poco sicuro di amministrare il proprio sistema, ma quando le reti locali erano ristrette a un ambito in cui tutto era comunque sotto controllo, la richiesta di una parola d'ordine poteva essere effettivamente un fastidio inutile.

Il riconoscimento può avvenire nel modo tradizionale, attraverso i file '`/etc/hosts.equiv`' e '`~/.rhosts`', oppure attraverso un'autenticazione Kerberos. Questo ultimo metodo non viene descritto.

Se si vuole concedere un accesso senza controlli particolari, si può predisporre il file '`/etc/hosts.equiv`' con un semplice elenco di nomi di nodi (o di indirizzi IP) a cui si concede l'accesso, in modo generalizzato, senza la richiesta di una parola d'ordine. Parallelamente, o alternativamente, ogni utente può predisporre il proprio elenco di nodi e di utenti da considerare equivalenti alla propria «identità» locale, preparando il file '`~/.rhosts`'.

L'esempio seguente mostra il contenuto del file '`/etc/hosts.equiv`' di un nodo per il quale si vuole consentire l'accesso da parte di *dinkel.brot.dg* e di *roggen.brot.dg*.

```
dinkel.brot.dg
roggen.brot.dg
```

In questo modo, gli utenti dei nodi *dinkel.brot.dg* e *roggen.brot.dg* possono accedere al sistema locale senza la richiesta formale di alcuna identificazione, purché esista per loro un'utenza con lo stesso nome.

L'elenco di nodi equivalenti può contenere anche l'indicazione di utenti particolari, per la precisione, ogni riga può contenere il nome di un nodo seguito eventualmente da **uno spazio** e dal nome di un utente. Si osservi l'esempio seguente:

```
dinkel.brot.dg
roggen.brot.dg
dinkel.brot.dg tizio
dinkel.brot.dg caio
```

Come nell'esempio precedente, viene concesso agli utenti dei nodi *dinkel.brot.dg* e *roggen.brot.dg* di accedere localmente se esistono utenze con lo stesso nome. In aggiunta a questo, però, viene concesso agli utenti '**`tizio`**' e '**`caio`**' del nodo *dinkel.brot.dg*, di accedere con **qualunque** nominativo-utente (locale), senza la richiesta di alcuna parola d'ordine.

Si può intuire che fare una cosa del genere significa concedere a tali utenti privilegi pericolosamente elevati. In generale, tali utenti non dovrebbero essere in grado di utilizzare numeri UID molto bassi, ma questo dipende da come sono stati compilati i sorgenti; comunque difficilmente ci può essere un buon motivo per configurare così il file '`/etc/hosts.equiv`'.

Il nome o l'indirizzo di un nodo può essere preceduto da un segno, '**`+`**' o '**`-`**', con il quale si intende, rispettivamente, includere

o escludere il nodo stesso. Come si può intendere, il segno '**+**' è predefinito.

Secondo la sintassi tradizionale di questo file, si può inserire una riga contenente soltanto il segno '**+**', allo scopo di **consentire l'accesso a qualunque nodo**. In questo senso si spiega poi la presenza del segno '**−**' per escludere qualche nodo particolare.

Come già accennato, indipendentemente dal fatto che il file '`/etc/hosts.equiv`' sia presente o meno, ogni utente può predisporre il proprio file '`~/.rhosts`'. La sintassi di questo file è la stessa di '`/etc/hosts.equiv`', ma si riferisce esclusivamente all'utente che predispone tale file nella propria directory personale. In questo file, l'indicazione di utenti precisi è utile e opportuna, perché quell'utente fisico, potrebbe essere riconosciuto con nomi differenti presso i nodi da cui vuole accedere.

```
dinkel.brot.dg tizi
roggen.brot.dg tizio
```

L'esempio mostra l'indicazione precisa di ogni nominativo-utente dei nodi che possono accedere senza richiesta di identificazione.[18]

I dettagli sull'uso di questi file possono essere differenti da un sistema all'altro. In particolare ci possono essere delle restrizioni ai permessi che può avere questo file; infatti, secondo il buon senso, '`/etc/hosts.equiv`' dovrebbe appartenere all'utente '**`root`**', senza consentire accessi in scrittura ad altri utenti; nello stesso modo, il file '`~/.rhosts`' dovrebbe appartenere all'utente al quale si riferisce, senza che altri possano avere permessi di scrittura su questo. Inoltre, dovrebbe essere impedito all'utente '**`root`**', così come agli

utenti speciali (cioè quelli corrispondenti a numeri UID particolarmente bassi), di accedere senza identificazione. Quindi, di solito, la sola configurazione del file '`/etc/hosts.equiv`' non basta a permettere l'accesso all'utente '**`root`**' senza che questo fornisca la parola d'ordine, anche se normalmente è sufficiente predisporre il file '`~root/.rhosts`'.[19] Si veda in ogni caso quanto descritto nelle pagine di manuale *hosts.equiv(5)* e *rhosts(5)*, se presenti nel proprio sistema.

36.7.1 Accesso remoto normale

L'accesso remoto tradizionale utilizza il protocollo LOGIN, si attua dal lato del servente con il demone '**`in.rlogind`**' (o solo '**`rlogind`**') e dal lato del cliente il programma '**`rlogin`**'. Il protocollo LOGIN è superato da TELNET (sezione 36.8). La sintassi per avviare demone dal lato del servente è molto semplice:

```
in.rlogind [opzioni]
```

Il demone '**`in.rlogin`**' va gestito dal supervisore dei servizi di rete e filtrato dal TCP wrapper. Nell'esempio seguente, viene mostrata la riga di '`/etc/inetd.conf`' in cui si dichiara il suo possibile utilizzo per quanto riguarda il caso particolare di Inetd:

```
login  stream  tcp  nowait  root  /usr/sbin/tcpd  in.rlogind
```

Opzione	Descrizione
`-h`	Permette anche all'utente '**`root`**' di utilizzare il file '`~/.rhosts`'.

Dal lato del cliente il programma '**`rlogin`**' consente di accedere

all'elaboratore remoto, come se ci si trovasse sulla console di quello:

```
rlogin [opzioni] nodo_remoto
```

Opzione	Significato mnemonico	Descrizione
`-l` ***utente***	*login*	Con questa opzione è possibile specificare già nella riga di comando il nome dell'utente da utilizzare per l'accesso nel sistema remoto. Quando ci si identifica in questo modo, viene richiesta la parola d'ordine in ogni caso.
`-8`		Abilita la connessione utilizzando una comunicazione a 8 bit in modo da poter utilizzare caratteri speciali che vanno oltre l'ASCII tradizionale.

36.7.2 Shell remota

Una shell remota è uno strumento per eseguire un comando in un elaboratore remoto dirigendo il flusso normale di dati attraverso il programma utilizzato localmente. Il protocollo usato originariamente per questo scopo è SHELL, superato da SSH (sezione 44.7). Per la gestione di una shell remota tramite il protocollo SHELL si utilizza il demone '**`in.rshd`**' (o '**`rshd`**') dal lato servente e '**`rsh`**' dal lato cliente.

Quando si utilizza una shell remota come Rsh, è importante fare mente locale alla sequenza delle operazioni che avvengono. Infatti, il comando viene interpretato inizialmente dalla shell locale che poi

passa gli argomenti a '**rsh**', il quale poi esegue un comando presso l'elaboratore remoto. Il problema sta quindi nel comprendere quale sia effettivamente il comando che viene poi eseguito nell'elaboratore remoto, tenendo conto anche della shell che viene utilizzata lì, per determinare il flusso di output che si ottiene (standard output e standard error), flusso che poi può essere visualizzato, ridiretto o rielaborato localmente.

Segue la sintassi per l'avvio del demone che offre questo servizio:

```
in.rshd [opzioni]
```

Il demone '**in.rshd**' va gestito dal supervisore dei servizi di rete e filtrato dal TCP wrapper ('**tcpd**'). Nell'esempio seguente, viene mostrata la riga di '`/etc/inetd.conf`' in cui si dichiara il suo possibile utilizzo per quanto riguarda il caso particolare di Inetd:

```
shell   stream  tcp   nowait  root   /usr/sbin/tcpd  in.rshd
```

Opzione	Descrizione
`-h`	Permette anche all'utente '**root**' di utilizzare il file '`~/.rhosts`'.

Dal lato del cliente il programma '**rsh**' permette di eseguire il comando richiesto nell'elaboratore remoto specificato se su quell'elaboratore è abilitata questa possibilità:

```
rsh [opzioni] nodo_remoto [comando]
```

Lo standard input ricevuto da '**rsh**' viene inviato allo standard input del comando remoto; lo standard output e lo standard error

emessi dal comando remoto vengono ridiretti in modo che diventino rispettivamente lo standard output e lo standard error di '**rsh**'.

Questo meccanismo di ridirezione è l'elemento che rende utile questo programma e d'altra parte è anche il suo limite: non possono essere utilizzati programmi che richiedono l'interazione con l'utente, attraverso '**rsh**'.

Se '**rsh**' viene utilizzata senza l'indicazione del comando remoto, si ottiene in pratica un accesso puro e semplice, attraverso '**rlogin**'.

Opzione	Significato mnemonico	Descrizione
`-l` ***utente***	*login*	Con questa opzione è possibile specificare già nella riga di comando il nome dell'utente da utilizzare per l'accesso nel sistema remoto. Quando ci si identifica in questo modo, viene richiesta la parola d'ordine in ogni caso.

Segue la descrizione di alcuni esempi per l'utilizzo di '**rsh**'.

- `$` **`rsh roggen.brot.dg cat /etc/fstab > copia-locale`**[*Invio*]

  Esegue il '**cat**' del file '`/etc/fstab`' dell'elaboratore *roggen.brot.dg* e ne dirige l'output verso il file locale '`copia-locale`'.

- `$` **`rsh roggen.brot.dg cat /etc/fstab ">" copia-remota`**[*Invio*]

  Questo esempio sembra molto simile al precedente, ma utilizzando il simbolo di ridirezione tra virgolette, la shell locale non lo interpreta in questo modo, ma lo lascia tra gli argomenti di '**rsh**'. Così facendo, il simbolo di ridirezione viene gestito

dal comando remoto generando il file ‘`copia-remota`’ proprio nell’elaboratore remoto.

- `$` **`rsh roggen.brot.dg tar czf - /home/pluto`** ↩
  ↪ **`> ~/pluto.tgz`** [*Invio*]

  Esegue l’archiviazione della directory ‘`/home/pluto/`’ dell’elaboratore *roggen.brot.dg* generando l’archivio compresso ‘`~/pluto.tgz`’ nell’elaboratore locale.

36.7.3 Copia tra elaboratori

«

Un modo per copiare dati tra un elaboratore e un altro può essere quello di sfruttare un file system di rete. Un altro modo potrebbe essere quello di utilizzare ‘**`rsh`**’ per copiare dati da un elaboratore remoto verso quello locale (viceversa è un po’ difficile) sfruttando il protocollo SHELL. In tal caso, il modo più pratico è rappresentato dall’utilizzo di ‘**`rcp`**’ attraverso il quale si possono copiare file tra due elaboratori remoti o tra un elaboratore remoto e quello locale.

Il programma ‘**`rcp`**’ si avvale di ‘**`rsh`**’, di conseguenza, dal lato servente occorre il demone ‘**`rshd`**’ e dal lato del cliente serve anche ‘**`rsh`**’. La sintassi per l’uso di ‘**`rcp`**’ ricalca in linea di massima quella di ‘**`cp`**’:

```
rcp [opzioni] origine destinazione
```

```
rcp [opzioni] origine... directory
```

I file o le directory indicati tra gli argomenti possono essere espressi nella forma seguente:

[[*utente* @] *nodo* :] *file*

Se non viene indicato esplicitamente un utente, si intende fare riferimento a un utente remoto con lo stesso nome di quello usato localmente; se non viene indicato il nome o l'indirizzo dell'elaboratore remoto, si intende quello locale.

Quando si fa riferimento a file remoti senza l'indicazione di un percorso assoluto, occorre tenere presente che la directory corrente di un elaboratore remoto corrisponde alla directory personale dell'utente a cui si fa riferimento. Nello stesso modo, occorre tenere presente che, dal momento che '**`rcp`**' si avvale di '**`rsh`**', le cose possono cambiare un po' a seconda del tipo di shell abbinato all'utente remoto.

Opzione	Significato mnemonico	Descrizione
`-r`	*recursive*	Se all'interno dei file indicati come origine della copia, si trovano anche directory, queste vengono copiate assieme al loro contenuto, in modo ricorsivo. In tal caso, necessariamente, la destinazione deve essere una directory.

Opzione	Significato mnemonico	Descrizione
`-p`	*preserve*	Con questa opzione si intende fare in modo che '**`rcp`**' tenti di riprodurre le stesse proprietà e gli stessi permessi nei file di destinazione, senza tenere conto del valore della maschera dei permessi (*umask*). Quando questa opzione non viene indicata, nel caso in cui il file di destinazione esista già, vengono mantenuti i permessi e le proprietà di quello esistente, mentre se i file di destinazione vengono creati, si utilizzano i permessi del file originale, filtrati attraverso la maschera dei permessi.

Seguono alcuni esempi.

- `$` **`rcp roggen.brot.dg:/home/tizio/letterina ./letterina`**[*Invio*]

  Copia il file '`/home/tizio/letterina`' contenuto nell'elaboratore *roggen.brot.dg*, nella directory corrente dell'elaboratore locale.

- `$` **`rcp roggen.brot.dg:\~/letterina ./letterina`**[*Invio*]

  Esegue un'operazione simile a quella dell'esempio precedente, ma in questo caso si utilizza un metacarattere, costituito dalla tilde, che deve essere interpretato dalla shell remota. Per evita-

re che la tilde venga invece interpretata dalla shell locale, viene utilizzata la barra obliqua inversa per proteggerla.

36.8 TELNET

TELNET è un protocollo che permette di effettuare un collegamento con un altro elaboratore e di operare su quello, come se si stesse utilizzando un suo terminale. Dal lato del servente occorre il demone '**telnetd**' (o meglio '**in.telnetd**'), mentre dal lato del cliente si utilizza normalmente il programma '**telnet**'.

Il cliente TELNET è molto importante anche come programma diagnostico per instaurare un collegamento manuale con una porta e iniziare quindi un colloquio diretto con il protocollo TCP. In questo caso, il demone '**telnetd**' non viene coinvolto.[20]

36.8.1 Dal lato del servente

Come già accennato, per eseguire un accesso in un elaboratore remoto attraverso il programma '**telnet**', è necessario che il demone '**in.telnetd**' sia in funzione in quell'elaboratore:

```
in.telnetd [opzioni]
```

Il demone '**in.telnetd**' è gestito normalmente dal supervisore dei servizi di rete e filtrato dal TCP wrapper. Nell'esempio seguente, viene mostrata la riga di '`/etc/inetd.conf`' in cui si dichiara il suo possibile utilizzo per quanto riguarda il caso particolare di Inetd:

```
…
telnet  stream  tcp  nowait  root  /usr/sbin/tcpd in.telnetd
…
```

Se è presente il file ‘`/etc/issue.net`’, viene utilizzato da ‘**`in.telnetd`**’ per visualizzare un messaggio introduttivo, non appena si instaura un collegamento. Si tratta di un file di testo con lo stesso ruolo del file ‘`/etc/issue`’ (14.15.2) che invece viene utilizzato da un programma Getty.

Il file ‘`/etc/issue.net`’ può contenere alcune sequenze di escape che vengono poi trasformate in vario modo nel momento della visualizzazione del messaggio. La tabella 36.102 ne mostra l’elenco.

Tabella 36.102. Elenco dei codici di escape utilizzabili all’interno del file ‘`/etc/issue.net`’.

Codice	Significato mnemonico	Descrizione
`%t`	*terminal*	Il terminale corrente.
`%h`	*host*	Il nome completo del sistema (FQDN).
`%D`	*domain*	Il nome del dominio NIS.
`%d`	*date*	La data e l’ora attuale.
`%s`	*system*	Il nome del sistema operativo.
`%m`	*machine*	Il tipo di hardware.
`%r`	*release*	Il rilascio del sistema operativo.

Codice	Significato mnemonico	Descrizione
`%v`	*version*	La versione del sistema operativo.
`%%`		Equivale a un carattere percentuale singolo.

36.8.2 Dal lato del cliente

L'accesso a un elaboratore remoto viene fatto principalmente attraverso il programma '**`telnet`**', il quale permette di operare come se ci si trovasse su un terminale di quel sistema:

```
telnet [opzioni] [nodo_remoto [porta] ]
```

Se l'eseguibile '**`telnet`**' viene avviato senza specificare il nodo con il quale ci si vuole connettere, questo inizia a funzionare in modalità di comando, visualizzando l'invito:

```
telnet>
```

Quando l'eseguibile '**`telnet`**' riesce a connettersi al sistema remoto, si opera come se si fosse seduti davanti a un terminale di quel sistema. Ma per poter dare dei comandi a '**`telnet`**' occorre tornare temporaneamente alla modalità di comando, cosa che si ottiene utilizzando il carattere di escape. Questo carattere di escape non corrisponde alla pressione del tasto [*Esc*], ma di solito alla combinazione [*Ctrl]*] (*control* + *parentesi quadra chiusa*). Tale convenzione può essere cambiata ed è una cosa quasi necessaria dal momento che utilizzando la tastiera italiana non è possibile ottenere le parentesi quadre se non in combinazione con [*AltGR*]. Diversamente, l'unico

modo per poter ottenere la combinazione [*Ctrl]*] è quello di passare a un'altra console virtuale, attivare la mappa della tastiera USA, tornare sulla console virtuale in cui è in funzione '**`telnet`**' ed eseguire la combinazione.

La comunicazione tra il cliente TELNET e il sistema remoto può essere di tre tipi:

TELNET LINEMODE	è il tipo preferito ed è il primo tipo di comunicazione che il cliente TELNET tenta di instaurare con il sistema remoto;
character at a time	in questa modalità ogni carattere viene trasmesso singolarmente al sistema remoto;
old line by line	i dati vengono trasmessi a blocchi di righe e ciò che viene scritto, riappare sul terminale locale.

Segue la descrizione di alcune opzioni e di alcuni argomenti della riga di comando.

Opzione o argomento	Significato mnemonico	Descrizione
`-4`		Richiede espressamente un collegamento con IPv4.
`-6`		Richiede espressamente un collegamento con IPv6.
`-8`		Tenta di negoziare una connessione a 8 bit.
`-d`	*debug*	Attiva inizialmente il controllo diagnostico.
`-a`	*auto*	Tenta di eseguire un accesso automatico.

Opzione o argomento	Significato mnemonico	Descrizione
`-n` ***file_traccia***		Registra le azioni effettuate durante il collegamento all'interno del file indicato.
`-l` ***utente***	*login*	Definisce il nominativo-utente da utilizzare per l'accesso nel sistema remoto.
`-e` ***carattere_di_escape***	*escape*	Permette di definire una sequenza diversa per il cosiddetto carattere di escape. Il valore predefinito è '**`^]`**' che non è tanto compatibile con la tastiera italiana.
nodo_remoto		Identifica il sistema remoto con il quale collegarsi. Può essere espresso in qualunque modo valido.
porta		Identifica il numero di porta (in forma numerica o attraverso il nome corrispondente). Se non viene specificato, si utilizza il valore predefinito per le connessioni TELNET: 23.

Segue la descrizione di alcuni dei comandi che possono essere usati in modo interattivo.

Comando	Descrizione
`close`	Chiude la connessione con l'elaboratore remoto.
`display` [***argomento***…]	Visualizza tutti o alcuni dei valori delle impostazioni che si possono definire attraverso il comando '**`set`**'.

Comando	Descrizione
`mode` ***tipo_di_modalità***	Permette di attivare una modalità particolare. L'attivazione della modalità richiesta dipende dal contesto e dalle possibilità offerte dal sistema remoto.
`mode character`	Attiva la modalità di comunicazione a un carattere alla volta.
`mode line`	Tenta di abilitare la modalità di comunicazione *TELNET LINEMODE*. Se non è possibile, si cerca di optare per la modalità *old line by line*.
`mode isig` `mode -isig`	Abilita o disabilita la modalità '**`TRAPSIG`**' che riguarda la comunicazione *TELNET LINEMODE*.
`mode edit` `mode -edit`	Abilita o disabilita la modalità '**`EDIT`**' che riguarda la comunicazione *TELNET LINEMODE*.
`mode softtab` `mode -softtab`	Abilita o disabilita la modalità '**`SOFT_TAB`**' che riguarda la comunicazione *TELNET LINEMODE*.
`mode litecho` `mode -litecho`	Abilita o disabilita la modalità '**`LIT_ECHO`**' che riguarda la comunicazione *TELNET LINEMODE*.
`mode ?`	Visualizza una breve guida per il comando '**`mode`**'.
`open` ***nodo_remoto*** ↩ ↪ [`-l` ***utente***] [***-porta***]	Apre una connessione con l'elaboratore remoto indicato. Se non viene specificata la porta, si utilizza il valore predefinito per le connessioni TELNET.

Comando	Descrizione
`quit`	Chiude la connessione (se esiste una connessione) e termina l'esecuzione di '**`telnet`**'. Durante la modalità di comando, è sufficiente premere la combinazione di tasti necessaria a ottenere il codice di EOF per terminare la sessione di lavoro.
`send` ***argomenti***	Permette di inviare uno o più sequenze di caratteri al sistema remoto.
`set` ***argomento valore` `unset*** ***argomento valore***	Il comando '**`set`**' attiva o specifica il valore di una variabile determinata, mentre '**`unset`**' disabilita o pone al valore di *Falso* la variabile specificata.
`!` [***comando***]	Permette di eseguire il comando indicato in una subshell all'interno del sistema locale.
`status`	Visualizza lo stato corrente della connessione.
`?` [***comando***]	Visualizza una breve guida del comando indicato o l'elenco dei comandi disponibili.

Se viene predisposto il file '`/etc/telnetrc`' a livello globale, o anche il file '`~/.telnetrc`' a livello personale, questi vengono letti quando si stabilisce un collegamento (naturalmente il secondo prevale sul primo). Se al loro interno appare un riferimento all'elaboratore con il quale ci si è collegati, vengono eseguite le istruzioni relative. Le righe che iniziano con il simbolo '**#**' sono commenti che terminano alla fine della riga. Le righe che non contengono spazi anteriori, dovrebbero iniziare con il nome di un nodo remoto; le righe successive che cominciano con almeno uno spazio, sono considerate come una serie di comandi da eseguire automaticamente all'atto

della connessione con quell'elaboratore.

36.8.3 Colloquiare con una porta

«

Un cliente TELNET è un ottimo strumento per eseguire una connessione TCP diagnostica con una porta di un nodo, sia remoto, sia locale. Naturalmente, per poter utilizzare questo sistema occorre conoscere il protocollo utilizzato dal demone con il quale ci si collega.[21]

L'esempio classico è l'invio di un messaggio di posta elettronica attraverso una connessione diretta con il servente SMTP. Dal file '`/etc/services`' si determina che il servizio SMTP (*Simple mail transfer protocol*) corrisponde alla porta 25, ma si può anche utilizzare semplicemente il nome '**`smtp`**'. Nell'esempio, si instaura un collegamento con il servente SMTP in funzione nel nodo *roggen.brot.dg*.

```
$ telnet roggen.brot.dg smtp [Invio]

  Trying 192.168.1.2...
  Connected to roggen.brot.dg.
  Escape character is '^]'.
  220 roggen.brot.dg ESMTP Sendmail 8.8.5/8.8.5; Thu, 11 Sep 1997 19:58:15 +0200
HELO brot.dg [Invio]

  250 roggen.brot.dg Hello dinkel.brot.dg [192.168.1.1], pleased to meet you
MAIL From: <daniele@dinkel.brot.dg> [Invio]

  250 <daniele@dinkel.brot.dg>... Sender ok
RCPT To: <toni@dinkel.brot.dg> [Invio]

  250 <toni@dinkel.brot.dg>... Recipient ok
```

DATA [*Invio*]

```
354 Enter mail, end with "." on a line by itself
```

Subject: Saluti. [*Invio*]

Ciao Antonio, [*Invio*]

come stai? [*Invio*]

Io sto bene e mi piacerebbe risentirti. [*Invio*]

Saluti, [*Invio*]

Daniele [*Invio*]

. [*Invio*]

```
250 TAA02951 Message accepted for delivery
```

QUIT [*Invio*]

```
221 dinkel.brot.dg closing connection
Connection closed by foreign host.
```

L'esempio mostrato dovrebbe funzionare senza bisogno di dare delle opzioni particolari all'eseguibile '**telnet**'; tuttavia, in certi casi può essere necessario l'uso dell'opzione '**-8**' per evitare che alcuni caratteri trasmessi o ricevuti possano essere alterati.

36.9 Trivial FTP

Il protocollo TFTP, o *Trivial FTP*, è un sistema di trasferimento di file senza autenticazione, paragonabile alla condivisione del file system attraverso il protocollo NFS. Si usa prevalentemente per consente l'avvio di sistemi senza disco (*diskless*).[22]

È importante sapere che questo tipo di servizio esiste, anche se non si intende sfruttare la possibilità di installare sistemi senza disco nella propria rete locale, eventualmente per sapere controllare che sia disattivato.

36.9.1 Dal lato del servente

Per poter offrire il servizio TFTP, occorre che nel servente sia disponibile il demone '**tftpd**' (o meglio '**in.tftpd**'), avviato generalmente attraverso il supervisore dei servizi di rete.

Data la debolezza di questo servizio che non richiede alcuna forma di identificazione da parte dei clienti, è necessario indicare una o più directory a partire dalle quali si consente di accedere. Se ciò non viene indicato, si fa riferimento a '`/tftpboot/`' in modo predefinito, ma è frequente la configurazione che utilizza la directory '`/var/lib/tftpboot/`':

```
in.tftpd [directory...]
```

Di solito si utilizza anche l'opzione '**-s**' per stabilire implicitamente che i percorsi assoluti richiesti si devono intendere successivi alla directory indicata come argomento o a '`/tftpboot/`' in sua mancanza:

```
in.tftpd -s [directory...]
```

Dal momento che il demone viene controllato dal supervisore dei servizi di rete, conviene controllare la configurazione di questo. L'esempio seguente si riferisce al file '`/etc/inetd.conf`'

per quanto riguarda il caso particolare di Inetd, dove si indica espressamente l'uso della directory '`/var/lib/tftpboot/`':

```
…
tftp dgram udp wait root /usr/sbin/tcpd ↩
↪in.tftpd -s /var/lib/tftpboot
…
```

36.9.2 Dal lato del cliente

Dal lato del cliente, l'uso del protocollo TFTP avviene probabilmente in modo implicito, all'interno di un'applicazione complessa che se ne avvale. Eventualmente, soprattutto per verificare il funzionamento di un servizio TFTP, è possibile utilizzare il programma '**`tftp`**' che viene mostrato qui.

Quando si effettua la connessione con un servente TFTP, non viene richiesta alcuna parola d'ordine e non viene eseguito alcun ***chroot()***; tuttavia è consentito l'accesso alle sole directory dichiarate nella riga di comando del demone corrispondente, oppure della sola '`/tftpboot/`'.

```
tftp [nodo]
```

Il programma '**`tftp`**' si comporta in modo simile a un cliente FTP (descritto nel capitolo 38), ma molto semplificato in confronto a quello. Il programma funziona in modo interattivo, attraverso una serie di comandi che vengono inseriti quando viene visualizzando l'invito:

```
tftp>
```

Eventualmente si può ottenere l'elenco dei comandi disponibili con il comando '**?**'.

A titolo di esempio viene mostrata la sequenza di una connessione ipotetica con il servente *dinkel.brot.dg*, allo scopo di prelevare una copia del file remoto '`/var/lib/tftpboot/192.168.1.10/etc/crontab`'. In questo caso, il demone '**tftpd**' è stato avviato senza l'opzione '**-s**':

```
$ tftp[Invio]

tftp> connect dinkel.brot.dg[Invio]

tftp> get /var/lib/tftpboot/192.168.1.10/etc/crontab↩
↪     /tmp/mio_crontab[Invio]

tftp> quit[Invio]
```

In questo caso, invece, il demone '**tftpd**' è stato avviato con l'opzione '**-s**':

```
$ tftp[Invio]

tftp> connect dinkel.brot.dg[Invio]

tftp> get /192.168.1.10/etc/crontab /tmp/mio_crontab[Invio]

tftp> quit[Invio]
```

36.10 Allineamento della data e dell'orario attraverso la rete

«

Il problema della sincronizzazione dell'orologio interno all'elaboratore con quello di altri nodi di rete può essere risolto almeno in due modi differenti: attraverso il protocollo TIME di Rdate e il proto-

collo NTP. Il protocollo NTP, a differenza di Rdate, si presta per la realizzazione di un sistema articolato di elaboratori che mantengono una sincronizzazione molto precisa tra di loro; in questo capitolo, il protocollo NTP viene visto solo per ottenere l'allineamento di un nodo di rete locale, con il quale si possono poi allineare gli altri nodi della propria rete, mentre si omette la descrizione della procedura necessaria a partecipare al sistema mondiale di gestione di questo servizio.

36.10.1 Rdate

Quasi tutti i nodi di rete hanno un orologio interno e offrono il servizio TIME attraverso la porta 37, come si vede dal file '`/etc/services`':

```
time    37/tcp  timeserver
time    37/udp  timeserver
```

In un sistema Unix tipico, questo servizio è offerto direttamente dal supervisore dei servizi di rete e nel caso di Inetd, il file di configurazione '`/etc/inetd.conf`' contiene normalmente la riga seguente:

```
time            stream  tcp     nowait  root    internal
```

Come si può osservare, non viene avviato alcun demone esterno per la sua gestione.

Per attingere al servizio, si usa normalmente Rdate, con l'eseguibile '**`rdate`**', che può prevedere la presenza di opzioni:

```
rdate [opzioni] nodo [porta]
```

In mancanza dell'indicazione del numero della porta da contattare presso il nodo remoto, si intende la porta 37; in mancanza di opzioni, si intende aggiornare l'orologio locale contestualmente all'interrogazione del servizio:

Opzione	Significato mnemonico	Descrizione
`-p`	*print*	Si limita a visualizzare la data e l'orario dell'elaboratore remoto.
`-s`	*set*	Si limita a impostare l'orologio locale con la data e l'orario dell'elaboratore remoto, senza visualizzare l'informazione.
`-a`	*adjust*	Imposta l'orologio locale in modo graduale.

Generalmente, non ci si limita a utilizzare Rdate per allineare l'orologio dell'elaboratore locale con quello di un nodo di rete remoto, ma si provvede anche ad aggiornare l'orologio hardware di conseguenza, come mostra l'esempio seguente:

```
# rdate dinkel.brot.dg[Invio]

  Mon May 12 17:04:21 2003
# clock -u -w[Invio]
```

Se al posto del programma '**clock**' si dispone di '**hwclock**', l'aggiornamento dell'orologio hardware si ottiene così:

```
# hwclock -u -w[Invio]
```

Come si vede, l'opzione '**-u**' implica che l'orologio hardware funzioni facendo riferimento al tempo universale.

Nella sezione successiva viene descritto l'uso del protocollo NTP; tuttavia, se dovesse risultare difficile ottenere accesso da un servente NTP pubblico, si può tentare di usare Rdate per ottenere l'ora esatta da un nodo, che si presume possa offrire un orario abbastanza esatto:

```
# rdate time.ien.it [Invio]
```

36.10.2 NTP

Il protocollo NTP (*Network time protocol*) consente di gestire una serie di nodi di rete in grado di sincronizzare tra loro l'orologio interno di ognuno.

La dipendenza dall'esterno per quanto riguarda la gestione degli orologi dei propri elaboratori, può costituire un problema di sicurezza. A questo proposito, il protocollo NTP offrirebbe anche la possibilità di utilizzare comunicazioni cifrate e altri sistemi di sicurezza; tuttavia qui non vengono considerati.

Per l'accesso a un servente NTP in qualità di cliente e per la gestione di servente in proprio, si utilizza di solito la «distribuzione NTP»,[23] rappresentata in pratica da un pacchetto che dovrebbe chiamarsi Ntp, o qualcosa del genere. I componenti più importanti di questa distribuzione sono il demone '**ntpd**' (oppure '**xntpd**') e il programma '**ntpdate**'.

36.10.2.1 Accesso a un servente NTP

«

Per lo scopo di questa sezione, si accede a un servente NTP solo per ottenere l'informazione sull'ora esatta. Ciò si ottiene molto facilmente con il programma '**ntpdate**', il quale è anche in grado di aggiustare l'orario del sistema. Tuttavia, prima di vedere come funziona, occorre sapere dove è possibile ottenere tale servizio e quali sono le regole di comportamento.

Trascurando i problemi legati alla gestione dei serventi NTP pubblici, quello che c'è da sapere è che questi sono organizzati in modo gerarchico a due strati. L'accesso ai serventi del primo strato è da escludere in generale, a meno che questo serva per gestire un servizio privato dal quale attingono un numero molto grande di altri clienti; l'accesso ai serventi del secondo strato è consentito quasi a tutti (ognuno ha però la sua politica) e in generale il risultato è accurato in modo più che sufficiente. Una volta chiarito che si accede di norma solo ai serventi di secondo livello, è opportuno sceglierne alcuni relativamente vicini (per quanto questo non sia indispensabile). L'elenco dei serventi NTP, con l'indicazione delle politiche rispettive, può essere trovato a partire dal sito *http://www.ntp.org* ; tuttavia, per le esigenze dell'utente finale tipico, è sufficiente fare riferimento all'indirizzo *pool.ntp.org*.

L'indirizzo *pool.ntp.org* si traduce in una serie di indirizzi IP alternativi, organizzati in modo tale che la trasformazione dell'indirizzo in nome generi ogni volta un indirizzo differente.

Ai fini degli esempi che si vogliono mostrare, viene utilizzato ripetutamente l'indirizzo *pool.ntp.org*. A titolo di verifica si può controlla-

re a cosa corrisponde; si potrebbe ottenere un elenco simile a quello che appare di seguito:

```
$ host pool.ntp.org [Invio]

  pool.ntp.org has address 203.109.252.7
  pool.ntp.org has address 206.168.231.98
  pool.ntp.org has address 213.96.80.106
  pool.ntp.org has address 213.239.193.168
  pool.ntp.org has address 216.165.129.244
  pool.ntp.org has address 24.34.79.42
  pool.ntp.org has address 62.101.81.203
  pool.ntp.org has address 62.212.114.68
  pool.ntp.org has address 65.211.109.11
  pool.ntp.org has address 69.17.92.121
  pool.ntp.org has address 129.240.64.3
  pool.ntp.org has address 130.60.7.44
  pool.ntp.org has address 130.94.201.36
  pool.ntp.org has address 198.144.202.250
  pool.ntp.org has address 202.74.170.194
```

Per acquisire l'ora esatta da uno o più serventi NTP e per aggiustare di conseguenza l'orario del sistema locale, si può usare '**ntpdate**':

```
ntpdate [opzioni] servente_ntp...
```

L'utilizzo di '**ntpdate**' è adatto particolarmente per gli elaboratori che sono connessi alla rete esterna solo saltuariamente, dal momento che si può effettuare l'allineamento esattamente nel momento in cui ciò è possibile. Con l'uso delle opzioni necessarie, si può evitare che '**ntpdate**' allinei l'orario del sistema, limitandosi a mostrare il risultato; in questi casi, può essere utilizzato anche dagli utenti comuni e non soltanto da '**root**'.

‘**ntpdate**’ non può essere avviato se è già in funzione il demone ‘**ntpd**’, o un altro analogo.

Tabella 36.119. Alcune opzioni della riga di comando di ‘**ntpdate**’.

Opzione	Significato mnemonico	Descrizione
`-b`		In condizioni normali, ‘**ntpdate**’ può scegliere di aggiustare l’orario aggiungendo o sottraendo secondi, oppure intervenendo sulla frequenza della base dei tempi. Per evitare che venga scelta la seconda ipotesi, si utilizza questa opzione, che limita la possibilità alla modifica dell’orario senza altri interventi. In condizioni normali, dovrebbe essere preferibile l’uso di ‘**ntpdate**’ con questa opzione.
`-d`	*debug*	Invece di allineare l’orario del sistema, vengono mostrati i passi compiuti da ‘**ntpdate**’, a scopo diagnostico.
`-q`	*query*	Invece di allineare l’orario del sistema, mostra solo il risultato dell’interrogazione dei serventi.

Opzione	Significato mnemonico	Descrizione
`-s`	*syslog*	Invece di mostrare i messaggi sullo schermo, li devia nel registro del sistema, cosa che facilita l'utilizzo di '**ntpdate**' all'interno di script avviati automaticamente in circostanze determinate.

Gli esempi seguenti completano la descrizione del funzionamento di '**ntpdate**'.

- `# ntpdate -q pool.ntp.org pool.ntp.org pool.ntp.org` [*Invio*]

  Visualizza l'ora esatta ottenuta da tre serventi ottenuti dallo stesso nome *pool.ntp.org*.

- `# ntpdate -b pool.ntp.org pool.ntp.org pool.ntp.org` [*Invio*]

  Aggiusta l'orario del sistema in base a quanto determinato da tre serventi *pool.ntp.org*.

- `# ntpdate -b -s pool.ntp.org pool.ntp.org pool.ntp.org` [*Invio*]

  Come nell'esempio precedente, con la differenza che ogni segnalazione viene inviata nel registro del sistema.

36.10.2.2 Preparazione di un servente NTP per l'utilizzo locale

La preparazione di un servente NTP per offrire il servizio solo alla propria rete locale, senza pretendere di contribuire alla rete NTP pubblica, è un'operazione abbastanza semplice. In particolare, se il nodo di rete che svolge tale ruolo è connesso continuamente alla rete

esterna, si può usare lo stesso demone '**ntpd**' per allineare l'orologio dell'elaboratore in cui si trova a funzionare, senza bisogno di utilizzare '**ntpdate**', considerato che questo non può essere avviato se è già attivo il demone.

Il funzionamento del demone '**ntpd**' dipende dalla configurazione stabilita attraverso il file '`/etc/ntp.conf`', mentre il programma '**ntpdate**' ignora questo file completamente.

Il file '`/etc/ntp.conf`' è il più importante per ciò che riguarda il funzionamento del demone '**ntpd**'. È composto da direttive che occupano ognuna una riga; i commenti sono preceduti dal simbolo '**#**' e nello stesso modo sono ignorate le righe bianche e quelle vuote. Senza entrare nel dettaglio delle varie direttive disponibili, viene descritto un esempio di massima.

```
# /etc/ntp.conf

logfile /var/log/xntpd
driftfile /var/lib/ntp/ntp.drift
statsdir /var/log/ntpstats/

statistics loopstats peerstats clockstats
filegen loopstats file loopstats type day enable
filegen peerstats file peerstats type day enable
filegen clockstats file clockstats type day enable

# Serventi
server pool.ntp.org
server pool.ntp.org
server pool.ntp.org
```

L'elenco seguente descrive alcune di queste direttive del file di

configurazione.

Direttiva	Descrizione
`logfile` ***file_delle_registrazioni***	Con la direttiva '**`logfile`**' viene dichiarato il percorso del file delle registrazioni. Se non venisse utilizzata tale direttiva, i messaggi di questo tipo sarebbero diretti normalmente al registro del sistema. Nel caso dell'esempio, si fa riferimento al file '`/var/log/xntpd`'.
`driftfile` ***file_dello_scarto***	Con la direttiva '**`driftfile`**' viene dichiarato il percorso del file utilizzato da '**`ntpd`**' per annotarsi lo scarto tra la frequenza dell'oscillatore locale e ciò che dovrebbe essere in realtà. Dal momento che '**`ntpd`**' deve poter cambiare nome al file e ricrearlo nuovamente, non può trattarsi di un collegamento simbolico. In generale, è sufficiente lasciare che sia '**`ntpd`**' a occuparsi di creare e gestire questo file.
`statsdir` ***directory_dei_file_statistici***	Con la direttiva '**`statsdir`**' viene dichiarato il percorso di una directory all'interno della quale possono essere creati dei file di informazioni statistiche, dichiarati a loro volta attraverso le direttive '**`statistics`**' e '**`filegen`**'.

Direttiva	Descrizione
`statistics` ***tipo_statistica***…	I tipi di informazioni statistiche che si vogliono accumulare sono definiti attraverso la direttiva '**`statistics`**', per mezzo di parole chiave prestabilite: '**`loopstats`**', '**`peerstats`**' e '**`clockstats`**'. In generale, conviene attivare la gestione di tutti i tipi di informazioni statistiche, così come si vede nell'esempio.

Direttiva	Descrizione
`filegen` ***tipo_statistica*** ↩ ↪ [`file` ***file***] ↩ ↪ [`type` ***tipo_di_analisi***] ↩ ↪ [`enable` | `disable`]	Per abbinare all'accumulo di un tipo di statistica un file vero e proprio, si utilizza la direttiva '**`filegen`**'. Nell'esempio vengono creati tre file, con il nome corrispondente al tipo di statistica di cui si occupano. Per la precisione, la direttiva '**`filegen`**' serve anche per definire il modo in cui vanno gestite diverse generazioni dei file che vengono creati. In pratica, il tipo stabilito attraverso l'argomento dell'opzione '**`type`**', permette di indicare con quale frequenza devono essere archiviati i file. L'esempio mostra la richiesta di utilizzare generazioni giornaliere (l'argomento '**`day`**') e questo, salvo esigenze particolari, dovrebbe andare bene in generale.

Direttiva	Descrizione
`server` ***nodo*** `[prefer]`	Le direttive più importanti per lo scopo che ci si prefigge in questo capitolo, sono quelle che stabiliscono i nomi dei serventi di riferimento per ottenere le informazioni sull'orario. In generale, più sono questi serventi, meglio è. Se uno di questi serventi viene considerato come quello più attendibile, si può aggiungere la parola chiave '**`prefer`**', come si vede nello schema sintattico.

Il demone '**`ntpd`**' (oppure '**`xntpd`**') serve da una parte per allineare continuamente l'orario del sistema locale, quando questo si trova connesso costantemente a una rete che gli consente di accedere ai suoi serventi di riferimento, in base alla configurazione del file '`/etc/ntp.conf`', con le direttive '**`server`**'. Dall'altra parte, questo demone offre anche il servizio NTP, basandosi sull'orologio del sistema locale:

```
ntpd [opzioni]
```

In una rete chiusa, in cui non ci sia la possibilità di raggiungere altri serventi NTP, il demone '**`ntpd`**' può essere utile per allestire il proprio servizio NTP locale, in modo da assicurare la sincronizzazione degli altri elaboratori della propria rete.

All'interno di questi due estremi, in una rete in cui un nodo abbia solo **saltuariamente** accesso alla rete esterna, quel nodo po-

trebbe essere allineato (quando possibile), al tempo di riferimento ottenuto dall'esterno, fungendo a sua volta da servente locale per l'allineamento successivo della propria rete. Tuttavia, in questo caso si aggiunge il problema di procedere all'allineamento in base alle fonti esterne, esattamente nel momento in cui il collegamento è disponibile; ma per questo si utilizza prevalentemente il programma '**ntpdate**' che però non può essere avviato quando il demone è già in funzione. Il problema si risolve evidentemente con uno script che, prima disattiva '**ntpd**', quindi allinea l'orario con '**ntpdate**', quindi rimette in funzione '**ntpd**'.

Opzione	Descrizione
`-c` ***file_di_configurazione***	In generale, il file di configurazione utilizzato da '**ntpd**' è '`/etc/ntp.conf`'. Con questa opzione si può indicare un file differente, oppure si può confermare la collocazione standard, nel caso i sorgenti siano stati compilati indicando posizioni differenti.
`-d`	La presenza di questa opzione, che può essere indicata anche ripetutamente, aumenta il livello di dettaglio delle informazioni diagnostiche che si ottengono (nel registro del sistema o in un altro file stabilito in base alla configurazione).
`-l` ***file_delle_registrazioni***	Equivalente alla direttiva '**logfile**' nel file di configurazione.
`-f` ***file_dello_scarto***	Equivalente alla direttiva '**driftfile**' nel file di configurazione.
`-s` ***directory_dei_file_statistici***	Equivalente alla direttiva '**statsdir**' nel file di configurazione.

L'esempio seguente mostra uno script molto semplificato per l'avvio e la conclusione del servizio NTP, attraverso il controllo del demone '**ntpd**'. In pratica, il demone viene avviato senza opzioni di alcun tipo, confidando che legga correttamente il file di configurazione.

```
#!/bin/sh

test -f /usr/sbin/ntpd || exit 0

case "$1" in
  start)
        printf "Avvio del servizio NTP: "
        /usr/sbin/ntpd
        echo
        ;;
  stop)
        printf "Disattivazione del servizio NTP: "
        killall ntpd
        echo
        ;;
  *)
        echo "Utilizzo: ntpd {start|stop}"
        exit 1
esac
```

Alcune distribuzioni GNU/Linux predispongono uno script del genere, in cui, prima dell'avvio del demone '**ntpd**' eseguono '**ntpdate**' per iniziare con un orologio già allineato. In generale, questa potrebbe essere una buona idea; tuttavia, se questo script viene avviato quando non si può accedere ai serventi NTP a cui si vuole fare riferimento, '**ntpdate**' blocca la procedura di avvio troppo a lungo.

Il pezzo di script che segue rappresenta proprio il caso in cui viene avviato anche '**ntpdate**' prima di mettere in funzione '**ntpd**'. Si osservi il fatto che nella riga di comando devono apparire i serventi NTP, perché il file di configurazione di '**ntpd**' non lo riguarda.

```
  start)
        printf "Avvio del servizio NTP: "
        /usr/sbin/ntpdate -b -s pool.ntp.org pool.ntp.org \
                              pool.ntp.org
        /usr/sbin/ntpd
        echo
        ;;
```

36.11 SNMP

Il protocollo SNMP (*Simple network management protocol*) ha lo scopo di consentire il controllo di apparecchiature raggiungibili attraverso la rete, fornendo un modo per pubblicare delle informazioni, che in parte possono anche essere rese modificabili.

Questa sezione introduce all'uso del protocollo SNMP, allo scopo di interrogare genericamente il servizio e di attivare un servente SNMP, utilizzando NET SNMP[24] in un sistema GNU/Linux. Viene invece omessa la spiegazione di come attivare delle «trappole».

36.11.1 Nomi delle variabili, OID e MIB

Le informazioni a cui è possibile accedere attraverso il protocollo SNMP sono strutturate ad albero, in modo tale da potervi fare riferimento attraverso l'indicazione di un percorso, secondo la forma '*... . a . b . c . ...*', dove al posto delle lettere (***a***, ***b***, ***c***, ecc.), possono apparire dei nomi (stringhe alfanumeriche per le quali non conta la distinzione tra maiuscole e minuscole) o dei valori numerici interi.

Naturalmente, l'associazione tra nomi e numeri, viene definita dagli standard che riguardano il protocollo SNMP.

Il percorso in questione si legge da sinistra verso destra, descrivendo con dettaglio sempre maggiore la variabile a cui si vuole fare riferimento. Un percorso «completo», inizia con un punto, a indicare la radice dell'albero che rappresenta la struttura complessiva delle variabili; un percorso che inizia senza punto, implica l'omissione di una porzione iniziale consueta del percorso stesso, costituita da: '`.iso.org.dod.internet.mgmt.mib-2.`', ovvero '`.1.3.6.1.2.1.`'.

I percorsi di esempio seguenti, sono da ritenere tutti uguali:

- '`.iso.org.dod.internet.mgmt.mib-2.system.sysDescr.0`'
- '`.1.3.6.1.2.1.1.sysdescr.0`'
- '`.1.3.6.1.2.1.1.1.0`'
- '`system.sysDescr.0`'
- '`1.sysdescr.0`'
- '`1.1.0`'

Nella terminologia usata per il protocollo SNMP, si fa spesso riferimento alla sigla OID (*Object identifier*). Un OID è un percorso qualunque di quelli che riguardano le variabili gestite dal protocollo, senza che debba arrivare necessariamente al dettaglio di una sola variabile. Per esempio, è un OID il percorso '`.iso.org.dod.internet.mgmt.mib-2.system`', il quale rappresenta tutto ciò che appartiene a quella gerarchia, ma è un OID anche un percorso che arriva fino in fondo, a specificare una sola variabile.

Gli «oggetti» (nel senso di OID) gestibili attraverso il protocollo SNMP, sono raggruppati a insiemi denominati MIB (*Management information base*).

36.11.2 Note essenziali sul protocollo

Il protocollo SNMP consente sostanzialmente di: richiedere a un servente la lettura di una certa variabile o di un gruppo di queste; modificare il contenuto delle variabili che il servente consente di alterare; di attivare delle «trappole» (*trap*) che scattino al verificarsi di certe condizioni, con le quali si vuole che alcune variabili (riferite al proprio nodo) siano inviate a un certo cliente SNMP.

Per queste funzioni, SNMP si avvale generalmente del protocollo UDP. Precisamente, per le operazioni di lettura e scrittura normali, ci si aspetta di trovare il servente in ascolto della porta 161 (161/UDP); invece, per l'invio di valori senza una richiesta preventiva (quando scattano delle trappole), ci si aspetta di trovare, presso la destinazione, un programma in ascolto della porta 162 (162/UDP).

Di norma, il servente SNMP viene chiamato «agente» (*agent*).

36.11.3 Autenticazione e limitazione degli accessi

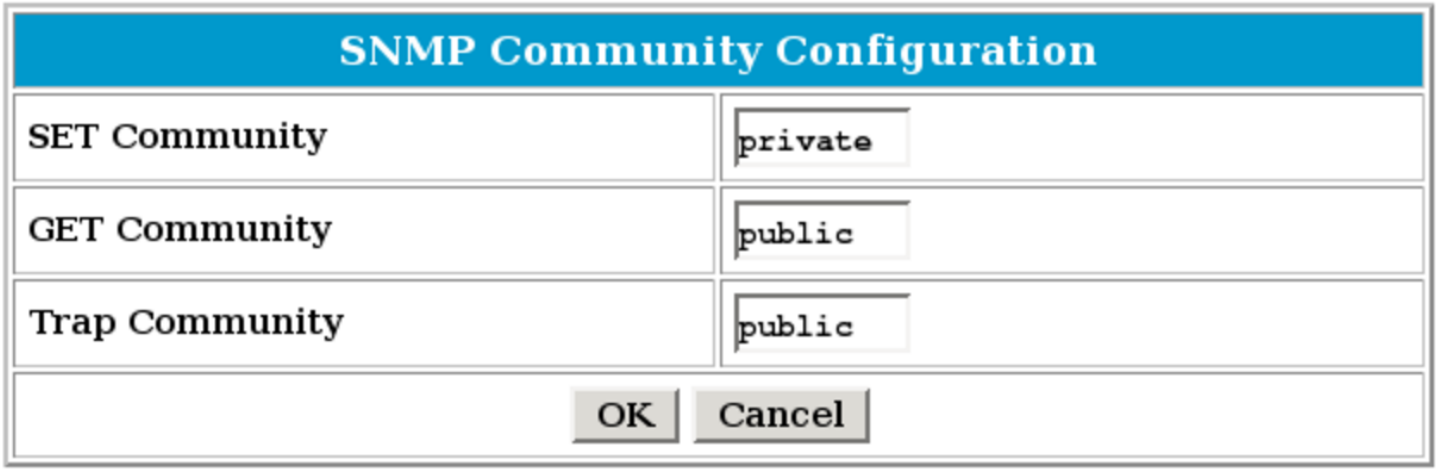
Il servente SNMP (ovvero l'agente) che riceve la richiesta di fornire delle informazioni, prima di rispondere, cerca di verificare che questa provenga da chi ha il diritto di ottenerle. Il servente può attuare una propria politica, basata sull'indirizzo di origine della richiesta (nel senso che si risponde solo a chi appartiene a un certo gruppo di indirizzi), ma nel protocollo stesso è prevista una qualche forma di riconoscimento.

Nelle versioni 1 e 2 del protocollo SNMP, il cliente si presenta al servente specificando il nome della «comunità» (*community*). In pratica, il servente risponde solo se il nome della comunità corrisponde a quello previsto (si distingue normalmente tra il nome da usare per la lettura delle variabili e quello da usare per la loro modifica). Tuttavia, occorre considerare che nella versione 1 del protocollo, il nome della comunità viene trasmesso in chiaro attraverso la rete, pertanto potrebbe essere individuato facilmente.

Nella versione 3 del protocollo SNMP, l'autenticazione può avvenire attraverso utenze e parole d'ordine individuali, ma questo meccanismo non viene descritto qui.

Notoriamente, la comunità predefinita, usata per la lettura delle variabili è '**`public`**', mentre quella per la scrittura è '**`private`**'. Naturalmente, è molto importante modificare questi nomi quando si attiva un servizio SNMP; inoltre, è altrettanto importante verificare se le apparecchiature connesse in rete offrono anche un servizio SNMP, provvedendo eventualmente a cambiare i nomi delle comunità anche se non si intende usufruirne.

Figura 36.125. Una pagina del programma di configurazione di un router VoIP, che consente l'uso del protocollo SNMP. La parola chiave '**SET**' si riferisce alla modifica delle variabili, mentre '**GET**' alla sola lettura.



Riquadro 36.126. Problemi di sicurezza.

È chiaro che l'attivazione di un servizio SNMP implichi la necessità di considerare come proteggere gli accessi, per non lasciare a chiunque di ottenere le informazioni relative. Ma è ancora più importante considerare che la maggior parte delle apparecchiature dedicate, collegate o collegabili alla rete, pubblicano delle informazioni attraverso il protocollo SNMP. In questi casi, dimenticare di modificare i nomi predefiniti delle comunità di lettura e scrittura, può essere fatale: alle volte vengono pubblicati in questo modo anche le parole d'ordine di accesso per la modifica della configurazione dell'apparecchio!

36.11.4 Interrogazione generica di un servizio SNMP

Il pacchetto NET SNMP[25] contiene diversi programmi per l'interrogazione di un servizio SNMP, le cui opzioni principali sono condivise. Per verificare che un servizio SNMP sia attivo, si usa normalmente '**snmpwalk**' o '**snmpbulkwalk**':

```
snmpwalk [opzioni] agente [percorso]
```

```
snmpbulkwalk [opzioni] agente [percorso]
```

Si osservi che nei modelli sintattici standard, al posto di ***percorso*** si indica la sigla OID. In pratica, il percorso non raggiunge necessariamente il dettaglio di una variabile singola.

La differenza tra i due programmi, sta nel fatto che il secondo ('**snmpbulkwalk**' si avvale specificatamente di funzionalità che sono disponibili a partire dalla versione 2 del protocollo SNMP, anche se il risultato apparente è lo stesso. Segue la descrizione di alcuni esempi.

- `$` **`snmpwalk -v 1 -c public localhost`**[*Invio*]

  Interroga il servizio SNMP presso l'elaboratore locale, utilizzando la versione 1 del protocollo e facendo riferimento alla comunità '**public**', che di solito è quella predefinita per la lettura delle variabili. Se il servizio risponde, si ottiene l'elenco di tutte le variabili disponibili:

```
SNMPv2-MIB::sysDescr.0 = STRING: Linux nanohost 2.6.17.1 ↩
↪#1 PREEMPT Fri Jun 30 21:44:31 CEST 2006 i686
SNMPv2-MIB::sysObjectID.0 = OID: SNMPv2-SMI::dod.0.0.0.0.0.0.0.0
SNMPv2-MIB::sysUpTime.0 = Timeticks: (207762) 0:34:37.62
…
…
IPV6-MIB::ipv6IfAdminStatus.7 = INTEGER: up(1)
IPV6-MIB::ipv6IfOperStatus.2 = INTEGER: up(1)
IPV6-MIB::ipv6IfOperStatus.7 = INTEGER: up(1)
```

Come si può osservare, in questo caso i percorsi delle variabili sono abbreviati attraverso l'indicazione del MIB di riferimento.

- `$` **`snmpwalk -O f -v 2c -c public localhost`**[*Invio*]

Rispetto all'esempio precedente, si richiede di visualizzare i percorsi secondo lo standard, usando i nomi rispettivi; inoltre si usa la versione 2 del protocollo.

```
.iso.org.dod.internet.mgmt.mib-2.system.sysDescr.0 = ↩
↪STRING: Linux nanohost 2.6.17.1 #1 PREEMPT ↩
↪Fri Jun 30 21:44:31 CEST 2006 i686
.iso.org.dod.internet.mgmt.mib-2.system.sysObjectID.0 = ↩
↪OID: .iso.org.dod.0.0.0.0.0.0.0
.iso.org.dod.internet.mgmt.mib-2.system.sysUpTime.0 = ↩
↪Timeticks: (227323) 0:37:53.23
…
…
.iso.org.dod.internet.mgmt.mib-2.ipv6MIB.ipv6MIBObjects.↩
↪ipv6IfTable.ipv6IfEntry.ipv6IfAdminStatus.7 = ↩
↪INTEGER: up(1)
.iso.org.dod.internet.mgmt.mib-2.ipv6MIB.ipv6MIBObjects.↩
↪ipv6IfTable.ipv6IfEntry.ipv6IfOperStatus.2 = ↩
↪INTEGER: up(1)
.iso.org.dod.internet.mgmt.mib-2.ipv6MIB.ipv6MIBObjects.↩
↪ipv6IfTable.ipv6IfEntry.ipv6IfOperStatus.7 = ↩
↪INTEGER: up(1)
```

- `$` **`snmpbulkwalk -O f -v 2c -c public localhost`**[*Invio*]

Si ottiene lo stesso risultato dell'esempio precedente.

- `$` **`snmpwalk -O n -v 2c -c public localhost`**[*Invio*]

Si ottengono i percorsi in forma numerica.

```
.1.3.6.1.2.1.1.1.0 = STRING: Linux nanohost 2.6.17.1 #1 ↩
↪PREEMPT Fri Jun 30 21:44:31 CEST 2006 i686
.1.3.6.1.2.1.1.2.0 = OID: .1.3.6.0.0.0.0.0.0.0
.1.3.6.1.2.1.1.3.0 = Timeticks: (263893) 0:43:58.93
…
…
.1.3.6.1.2.1.55.1.5.1.9.7 = INTEGER: up(1)
.1.3.6.1.2.1.55.1.5.1.10.2 = INTEGER: up(1)
.1.3.6.1.2.1.55.1.5.1.10.7 = INTEGER: up(1)
```

- `$ snmpwalk -O n -v 2c -c public localhost ↩`
  `↪ .1.3.6.1.2.1.1.9.1` [*Invio*]

  Si ottengono le variabili, limitatamente a un certo OID.

```
.1.3.6.1.2.1.1.9.1.2.1 = OID: .1.3.6.1.2.1.31
.1.3.6.1.2.1.1.9.1.2.2 = OID: .1.3.6.1.6.3.1
.1.3.6.1.2.1.1.9.1.2.3 = OID: .1.3.6.1.2.1.49
…
.1.3.6.1.2.1.1.9.1.4.7 = Timeticks: (10) 0:00:00.10
.1.3.6.1.2.1.1.9.1.4.8 = Timeticks: (10) 0:00:00.10
.1.3.6.1.2.1.1.9.1.4.9 = Timeticks: (10) 0:00:00.10
```

Per leggere in modo particolare una sola variabile, si usa normalmente '**snmpget**' o '**snmpgetnext**':

```
snmpget [opzioni] nodo variabile
```

```
snmpgetnext [opzioni] nodo variabile
```

Il risultato ottenuto dai due programmi è diverso, in quanto il primo mostra il contenuto della variabile indicata, mentre il secondo mostra quella successiva a quella indicata. Segue la descrizione di alcuni

esempi, omettendo di precisare dettagli già descritti a proposito di quelli su '**snmpwalk**' e '**snmpbulkwalk**', in quanto le opzioni usate sono equivalenti.

- `$` **`snmpget -O n -v 2c -c public localhost`** ↩
  ↪ **`.1.3.6.1.2.1.1.1.0`**[*Invio*]

  Interroga la variabile ***.iso.org.dod.internet.mgmt.mib-2.system.sysDe***

```
.1.3.6.1.2.1.1.1.0 = STRING: Linux nanohost 2.6.17.1 #1 ↩
↪PREEMPT Fri Jun 30 21:44:31 CEST 2006 i686
```

- `$` **`snmpgetnext -O n -v 2c -c public localhost`** ↩
  ↪ **`.1.3.6.1.2.1.1.9.1.3.9`**[*Invio*]

  Interroga la variabile successiva a '`.iso.org.dod.internet.mgmt.mib-2.system.sysORTable.sysOREntry.sysORDescr.9`', che in questo caso corrisponde a '`.iso.org.dod.internet.mgmt.mib-2.system.sysORTable.sysOREntry.sysORUpTime.1`'.

```
.1.3.6.1.2.1.1.9.1.4.1 = Timeticks: (10) 0:00:00.10
```

Tabella 36.133. Alcune opzioni comuni nei programmi di NET SNMP.

Opzione	Descrizione
`-v 1|2c|3`	Specifica la versione del protocollo SNMP da utilizzare.
`-c` ***comunità***	Specifica il nome della comunità a cui fare riferimento e si applica solo alle versioni 1 e 2 del protocollo.
`-O f`	Mostra il percorso utilizzando i nomi.
`-O n`	Mostra il percorso in forma numerica.

36.11.5 Interrogazioni più specifiche di un servizio SNMP

«

Il pacchetto NET SNMP[26] include anche qualche programma per l'interrogazione di un servizio SNMP, in riferimento a problemi specifici, mostrando il risultato in un modo conforme al problema stesso. Naturalmente, perché questi programmi possano mostrare le informazioni richieste, occorre che il servizio SNMP pubblichi le variabili necessarie.

```
snmpdf [opzioni] nodo
```

Il programma '**snmpdf**' consente di ottenere informazioni sullo spazio utilizzato e disponibile nei dischi. In pratica, la sigla '**df**' fa volutamente riferimento al programma di un sistema Unix che di solito compie questa funzione. L'esempio seguente dovrebbe essere più che sufficiente per comprenderne il funzionamento:

```
$ snmpdf -v 2c -c public localhost[Invio]

 Description          size (kB)          Used     Available Used%
 Memory Buffers          513204         50168        463036    9%
 Real Memory             513204        499240         13964   97%
 Swap Space             5148856           796       5148060    0%
 /                     40679248      21106328      19572920   51%
 /sys                         0             0             0    0%
 /proc/bus/usb                0             0             0    0%
 /home                193540640      98867424      94673216   51%
```

Attraverso '**snmpnetstat**' è possibile interrogare lo stato delle connessioni, come si farebbe con il programma '**netstat**':

```
snmpnetstat [opzioni] nodo
```

Oltre alle opzioni comuni di NET SNMP, altre consentono di limitare la visualizzazione a una porzione di proprio interesse. L'esempio seguente esegue semplicemente un'interrogazione complessiva, visualizzando gli indirizzi in forma numerica (opzione '**-n**'):

```
$ snmpnetstat -v 2c -c public -n localhost[Invio]

  Active Internet (tcp) Connections
  Proto Local Address          Remote Address         (state)
  tcp   127.0.0.1.4221         127.0.0.1.5901        ESTABLISHED
  tcp   127.0.0.1.5901         127.0.0.1.4221        ESTABLISHED
  tcp   172.21.77.5.707        172.21.254.254.861    TIMEWAIT
  tcp   172.21.77.5.1023       172.21.254.254.2049   ESTABLISHED
  tcp   172.21.77.5.1651       62.123.24.21.22       ESTABLISHED
  tcp   172.21.77.5.3865       172.21.254.254.111    TIMEWAIT
  tcp   172.21.77.5.4165       62.123.24.21.22       ESTABLISHED
  Active Internet (udp) Connections
  Proto Local Address
  udp   *.9
  udp   *.69
  udp   *.111
  udp   *.137
  udp   *.138
  udp   *.514
  udp   *.623
  udp   *.638
  udp   *.812
  udp   *.924
  udp   *.1025
  udp   *.1028
  udp   *.1031
```

```
udp    *.1048
udp    *.2049
udp    *.3130
udp    *.9676
udp    127.0.0.1.53
udp    127.0.0.1.161
udp    172.21.77.5.53
udp    172.21.77.5.137
udp    172.21.77.5.138
```

Con '**snmpstatus**' è possibile ottenere alcune informazioni statistiche:

```
snmpstatus [opzioni] nodo
```

Ecco un esempio comune:

```
$ snmpstatus -v 2c -c public localhost[Invio]

 [UDP: [127.0.0.1]:161]=>[Linux nanohost 2.6.17.1 #1 ↩
↪PREEMPT Fri Jun 30 21:44:31 CEST 2006 i686] Up: ↩
↪0:52:13.49
 Interfaces: 7, Recv/Trans packets: 451271/401702 | ↩
↪IP: 451199/401542
 5 interfaces are down!
```

36.11.6 Attivazione di un servizio SNMP con NET SNMP

«

NET SNMP include un demone per offrire un servizio SNMP presso un elaboratore:

```
snmpd [opzioni]
```

Di norma, questo programma viene avviato attraverso la procedura di inizializzazione del sistema, pertanto si interviene con script appositi del proprio sistema operativo (per esempio '`/etc/init.d/snmpd`'). Inoltre, il file di configurazione dovrebbe essere '`/etc/snmp/snmpd.conf`'.

La predisposizione del file di configurazione non è semplice; di solito si parte da quello già predisposto dalla propria distribuzione del sistema operativo, attraverso modifiche più o meno intuitive, contando sulle descrizioni contenute nei commenti. Tuttavia, eventualmente, se le proprie esigenze sono limitate al controllo degli accessi in modo semplificato, è possibile utilizzare il programma '**snmpconf**' per generare un file di configurazione, da zero. Segue un esempio per ottenere semplicemente la configurazione degli accessi in sola lettura a partire dall'elaboratore locale:

```
$ snmpconf -g basic_setup[Invio]

  The following installed configuration files were found:

     1:  /etc/snmp/snmpd.conf

  Would you like me to read them in?  Their content will be
  merged with the output files created by this session.

  Valid answer examples: "all", "none","3","1,2,5"

Read in which (default = all): all[Invio]

  ***********************************************
  *** Beginning basic system information setup ***
  ***********************************************
```

```
Do you want to configure the information returned in the ↩
↪system MIB group (contact info, etc)? (default = y): y[Invio]

  Configuring: syslocation
  Description:
    The [typically physical] location of the system.
      Note that setting this value here means that when trying
      to perform an snmp SET operation to the sysLocation.0
      variable will make the agent return the "notWritable"
      error code.  IE, including this token in the snmpd.conf
      file will disable write access to the variable.
      arguments:  location_string

The location of the system: ufficio[Invio]

  Configuring: syscontact
  Description:
    The contact information for the administrator
      Note that setting this value here means that when trying
      to perform an snmp SET operation to the sysContact.0
      variable will make the agent return the "notWritable"
      error code.  IE, including this token in the snmpd.conf
      file will disable write access to the variable.
      arguments:  contact_string

The contact information: tizio@brot.dg[Invio]

  Finished Output: syscontact  tizio@brot.dg

Do you want to properly set the value of the ↩
↪sysServices.0 OID ↩
↪(if you don't know, just say no)? (default = y): n[Invio]

  ************************************
  *** BEGINNING ACCESS CONTROL SETUP ***
  ************************************
```

```
Do you want to configure the agent's access control? ↩
↪(default = y): y[Invio]

Do you want to allow SNMPv3 read-write user based access ↩
↪(default = y): n[Invio]

Do you want to allow SNMPv3 read-only user based access ↩
↪(default = y): n[Invio]

Do you want to allow SNMPv1/v2c read-write community access ↩
↪(default = y): n[Invio]

Do you want to allow SNMPv1/v2c read-only community access
(default = y): y[Invio]

  Configuring: rocommunity
  Description:
    a SNMPv1/SNMPv2c read-only access community name
      arguments:  community [default|hostname|network/bits] [oid]


The community name to add read-only access for: public[Invio]

The hostname or network address to accept this community ↩
↪name from [RETURN for all]: 127.0.0.1[Invio]

The OID that this community should be restricted to ↩
↪[RETURN for no-restriction]: [Invio]

  Finished Output: rocommunity  public 127.0.0.1


Do another rocommunity line? (default = y): n[Invio]

  ****************************************
  *** Beginning trap destination setup ***
  ****************************************


Do you want to configure where and if the agent will send ↩
```

```
↪traps? (default = y): n[Invio]

  ***********************************
  *** Beginning monitoring setup ***
  ***********************************


Do you want to configure the agent's ability to monitor ↩
↪various aspects of your system? (default = y): n[Invio]

  The following files were created:

    snmpd.conf

  These files should be moved to …
  …
```

In pratica, al termine dell'esempio, si ottiene il file '`snmpd.conf`' nella directory corrente, che l'utente può copiare probabilmente in '`/etc/snmp/`', o in una posizione analoga, in base all'impostazione del proprio sistema. Ecco il contenuto del file, omettendo tutti i commenti:

```
syslocation  ufficio
syscontact  tizio@brot.dg
rocommunity  public 127.0.0.1
```

Naturalmente, soprattutto se si intende offrire l'accesso a elaboratori esterni, può essere conveniente cambiare il nome della comunità.

36.11.7 MRTG

«

MRTG[27] è un programma in grado di interrogare un router che disponga di un servizio SNMP, per disegnare automaticamente dei grafici sul traffico che lo riguarda. I grafici in questione vengono ac-

compagnati da una pagina HTML che guida all'interpretazione dei valori, facilitandone così la pubblicazione.

36.11.7.1 Configurazione

Per usare MRTG è indispensabile predisporre un file di configurazione, collocabile ovunque, ma in generale potrebbe corrispondere a '`/etc/mrtg.cfg`'. Per costruire correttamente questo file occorre conoscere perfettamente le caratteristiche del router (o comunque del nodo di rete) da tenere sotto controllo, ma in pratica ci si avvale di un programma apposito che esplora le caratteristiche dell'agente SNMP da considerare, quindi scrive una configurazione valida. Il programma in questione è '**`cfgmaker`**':

```
cfgmaker [opzioni] agente_snmp...
```

L'agente SNMP si indica secondo la forma consueta:

```
[comunità@] nodo
```

In pratica, se si omette il nome della comunità, si intende '**`public`**'.

Tabella 36.149. Alcune opzioni per l'utilizzo di '**`cfgmaker`**'.

Opzione	Descrizione
`--enable-ipv6`	Abilita l'uso di IPv6.
`--output=`*file*	Dichiara il file di configurazione da creare automaticamente. In mancanza di questa indicazione, il risultato viene emesso attraverso lo standard output.

Opzione	Descrizione
`--zero-speed=`***n_bit_s***	Se dall'interrogazione SNMP risulta che un'interfaccia opera a velocità zero, si fa in modo che si consideri invece il valore indicato con l'opzione, che si intende esprimere una quantità di bit per secondo.

Segue la descrizione di alcuni esempi.

- # **`cfgmaker localhost mia@172.17.1.1 > /etc/mrtg.cfg`**[*Invio*]

  Genera il file '`/etc/mrtg.cfg`', contenente le direttive necessarie a controllare tutte le interfacce di rete attive nell'elaboratore locale (*localhost*), utilizzando la comunità predefinita ('**`public`**'), e quelle dell'elaboratore raggiungibile con l'indirizzo 172.17.1.1, utilizzando in questo caso la comunità '**`mia`**'.

- # **`cfgmaker --output=/etc/mrtg.cfg localhost`** ↩
  ↪ **`mia@172.17.1.1`**[*Invio*]

  Genera il file '`/etc/mrtg.cfg`', esattamente come nell'esempio precedente.

- # **`cfgmaker --enable-ipv6 localhost mia@172.17.1.1`** ↩
  ↪ **`> /etc/mrtg.cfg`**[*Invio*]

  Come nell'esempio precedente, abilitando l'uso di IPv6.

Il file di configurazione che si ottiene, contiene anche direttive che potrebbe essere necessario cambiare, per le proprie esigenze contingenti. In particolare è importante accertarsi che i grafici da produrre vengano creati nella directory che ci si aspetta sia usata per questo:

```
...
WorkDir: /var/www/mrtg
...
```

In questo caso MRTG viene istruito per mettere i file che crea nella directory '`/var/www/mrtg/`'. Eventualmente, si può fare in modo che sia '**`cfgmaker`**' che predispone questa direttiva nel modo che più si preferisce, senza dover ritoccare a mano il file di configurazione, attraverso l'opzione speciale '**`--global`**':

```
# cfgmaker --enable-ipv6 ↩
↪          --global="WorkDir: /var/www/mrtg" ... ↩
↪          > /etc/mrtg.cfg [Invio]
```

36.11.7.2 Utilizzo del programma

Quando si dispone di un file di configurazione, si può utilizzare MRTG per interrogare i vari agenti SNMP previsti, a intervalli regolari:

```
mrtg [opzioni] file_di_configurazione
```

Di solito non si usano opzioni, indicando semplicemente il file di configurazione a cui fare riferimento. Piuttosto, la cosa più importante da considerare è il fatto che il programma non accetta altra configurazione locale che quella tradizionale dei sistemi Unix: '**`C`**'. In pratica, va usato così:

```
LANG=C mrtg [opzioni] file_di_configurazione
```

Ovvero:

```
env LANG=C mrtg [opzioni] file_di_configurazione
```

Il programma va eseguito a intervalli regolari, attraverso Cron; di solito lo si fa con una cadenza di cinque minuti. Ecco come si potrebbe configurare Cron al riguardo (sezione 11.5):

```
...
*/5 * * * * root if [ -x /usr/bin/mrtg ]  ↩
↪                    && [ -r /etc/mrtg.cfg ]; ↩
↪                  then env LANG=C /usr/bin/mrtg ↩
↪                    /etc/mrtg.cfg ↩
↪                       >> /var/log/mrtg/mrtg.log 2>&1; fi
...
```

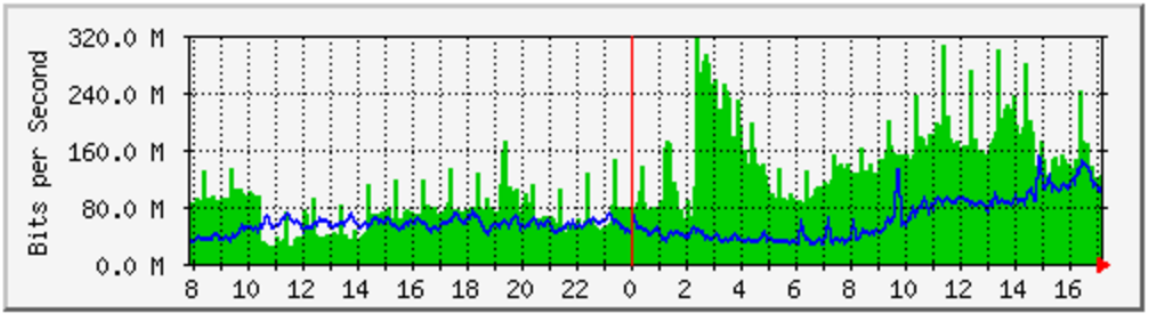
36.11.7.3 Il risultato

«

In base alla configurazione, il programma '**mrtg**' va a memorizzare i dati letti presso i vari agenti SNMP previsti, all'interno di file contenuti nella directory stabilita come '**WorkDir**' (per esempio '`/var/www/mrtg/`'. Inoltre, ogni volta, sulla base dei dati accumulati, produce i grafici in forma di file PNG, accompagnati da un file HTML che ne facilita la lettura. Ecco come potrebbe apparire uno di questi grafici, visto attraverso la pagina HTML di riferimento:

The statistics were last updated **Monday, 31 July 2006 at 17:10**, at which time **'rou-rz-gw.ethz.ch'** had been up for **84 days, 6:24:51**.

`Daily' Graph (5 Minute Average)



	Max	Average	Current
In	319.4 Mb/s (7.4%)	110.3 Mb/s (2.6%)	124.2 Mb/s (2.9%)
Out	149.3 Mb/s (3.5%)	57.8 Mb/s (1.3%)	110.1 Mb/s (2.6%)

36.12 Rsync

Rsync[28] è un sistema di copia tra elaboratori (o anche all'interno del file system dello stesso sistema locale), in grado di individuare e trasferire il minimo indispensabile di dati, allo scopo di allineare la destinazione con l'origine. L'uso di questo programma è molto semplice ed è simile a quello di '**`rcp`**' (*Remote shell copy*) o anche di '**`scp`**' (*Secure shell copy*).

L'aggiornamento dei dati, in funzione delle opzioni utilizzate, può basarsi sul confronto delle date di modifica, delle dimensioni dei file e anche sul calcolo di un codice di controllo (*checksum*). In linea di principio, a meno di utilizzare opzioni che specificano qualcosa di diverso, non conta il fatto che i dati siano più recenti o meno, basta che questi siano diversi per ottenerne il trasferimento.

36.12.1 Tipi di utilizzo

«

Rsync può utilizzare diverse modalità di trasferimento dei file, a seconda delle circostanze e delle preferenze. Per la precisione si distinguono tre possibilità fondamentali.

Copia locale

In tal caso, la copia, o l'allineamento, avviene all'interno dello stesso sistema, dove l'origine e la destinazione sono riferite semplicemente a posizioni differenti nel file system. In questa circostanza, Rsync viene utilizzato come metodo evoluto di copia.

Copia tra elaboratori attraverso '**rsh**' o simili

Si tratta di un'operazione che coinvolge due elaboratori differenti, anche se uno dei due deve essere necessariamente quello locale, in cui il trasferimento dei dati avviene attraverso '**rsh**' o un suo equivalente (come '**ssh**'), utilizzando una copia del programma '**rsync**' anche nell'elaboratore remoto.

Copia tra elaboratori attraverso un protocollo specifico di Rsync

Si tratta di un sistema di copia tra elaboratori, dove in quello remoto si trova in funzione una copia del programma '**rsync**', avviata in modo che resti in ascolto della porta TCP 873. In questo caso, la connessione tra elaboratore locale ed elaboratore remoto avviene direttamente senza l'utilizzo di una shell per l'accesso remoto.

36.12.2 Origine, destinazione e percorsi

La forma utilizzata per esprimere l'origine e la destinazione permette di distinguere anche la modalità con cui si vuole che la copia o l'allineamento siano eseguiti.

Sintassi	Descrizione
percorso	L'assenza del simbolo di due punti (':'), indica che si tratta di un percorso riferito al file system locale.
[***utente*** `@`] ***nodo*** `:` ***percorso***	La presenza di un simbolo di due punti singolo (':'), indica che si tratta di un percorso riferito a un nodo remoto e che per la connessione si vuole usare una shell per l'accesso remoto.
[***utente*** `@`] ***nodo*** `::` ***percorso*** `rsync://` [***utente*** `@`] ***nodo*** `/` ***percorso***	La presenza di un simbolo di due punti doppio ('::'), o l'indicazione esplicita del protocollo Rsync (*rsync://*), indica che si tratta di un percorso riferito a un nodo remoto e che per la connessione si vuole usare il protocollo specifico di Rsync.

L'indicazione dei percorsi merita attenzione. Per prima cosa si può dire che valgono regole simili a quelle della copia normale; per cui, si può copiare un file singolo, anche indicando espressamente il nome che si vuole nella destinazione (che potrebbe essere diverso da quello di origine); inoltre si possono copiare uno o più file e directory in una destinazione che sia una directory.

- Quando l'origine è locale, si possono indicare diversi percorsi, anche con l'aiuto di metacaratteri (caratteri jolly) che poi vengono interpretati opportunamente ed espansi dalla shell locale. L'esempio seguente, mostra il comando necessario a copiare o ad allineare i file che terminano per '`.sgml`', della directory corrente, con quanto contenuto nella directory '`/tmp/prove/`' del nodo *roggen.brot.dg*.

  ```
  $ rsync *.sgml roggen.brot.dg:/tmp/prove [Invio]
  ```

- Quando l'origine è remota, si possono indicare diversi percorsi, anche con l'aiuto di metacaratteri che poi vengono interpretati opportunamente ed espansi dalla shell utilizzata nell'utenza remota. La differenza sta nel fatto che i metacaratteri utilizzati non devono essere interpretati dalla shell locale, per cui è bene usare delle tecniche di protezione adatte. Probabilmente, ciò non è indispensabile, perché alcune shell come Bash ignorano l'espansione dei nomi se questi non possono avere una corrispondenza nel file system locale.

  L'esempio seguente, mostra il comando necessario a copiare o ad allineare i file che terminano per '`.sgml`', della directory '`/tmp/prove/`' del nodo *roggen.brot.dg*, con quanto contenuto nella directory corrente dell'elaboratore locale.

  ```
  $ rsync 'roggen.brot.dg:/tmp/prove/*.sgml' . [Invio]
  ```

- Quando l'origine fa riferimento a una directory, ma **non** si utilizza la barra obliqua finale, si intende individuare la directory, come se fosse un file normale. La directory di origine viene copiata nella directory di destinazione, aggiungendola a questa. Per cui, l'esempio seguente serve a copiare la directory locale

'`/tmp/ciao/`' nella directory remota '`/tmp/prove/`', generando '`/tmp/prove/ciao/`' e copiando al suo interno i file e le sottodirectory che fossero eventualmente contenuti nel percorso di origine.

```
$ rsync -r /tmp/ciao roggen.brot.dg:/tmp/prove [Invio]
```

- Quando l'origine fa riferimento a una directory e si utilizza la barra finale, si intende individuare tutto il **contenuto** della directory, escludendo la directory stessa. Per cui, l'esempio seguente serve a copiare il contenuto della directory locale '`/tmp/ciao/`' nella directory remota '`/tmp/prova/`', generando eventuali file e sottodirectory contenuti nella directory di origine.

```
$ rsync -r /tmp/ciao/ roggen.brot.dg:/tmp/prove [Invio]
```

È diverso copiare il contenuto di una directory dal copiare una directory intera (assieme al suo contenuto); nel primo caso, si rischia di perdere la copia dei file «nascosti», ovvero quelli che iniziano con un punto.

36.12.3 Proprietà dei file

Come è possibile vedere in seguito, quando si utilizzano le opzioni '**-o**' ('**--owner**') e '**-g**' ('**--group**'), si intende fare in modo che nella destinazione sia mantenuta la stessa proprietà dei file (dell'utente o del gruppo) che questi hanno nell'origine.

Per ottenere questo risultato, si confrontano generalmente i nomi degli utenti e dei gruppi, assegnando i numeri UID e GID necessari. Quando questa corrispondenza dovesse mancare, viene utilizzato

semplicemente lo stesso numero ID. In alternativa, con l'uso dell'opzione '**--numeric-ids**', si può richiedere espressamente l'uguaglianza numerica di UID o GID, indipendentemente dai nomi utilizzati effettivamente.

36.12.4 Avvio del programma

Il programma eseguibile '**rsync**' è quello che svolge tutte le funzioni necessarie ad allineare una destinazione, in base al contenuto di un'origine. Per questo, come già chiarito, si può avvalere di '**rsh**', di un'altra shell per l'accesso remoto o di un servente Rsync remoto.

```
rsync [opzioni] origine destinazione
```

L'origine e la destinazione possono essere riferite indifferentemente al nodo locale o a un nodo remoto. Quello che conta è che almeno una delle due sia riferita al nodo locale.

Tabella 36.154. Alcune opzioni.

Opzione	Descrizione
`-v` `--verbose`	Permette di ottenere più informazioni sullo svolgimento delle operazioni. Questa opzione può essere usata più volte, incrementando il livello di dettaglio di tali notizie.
`-q` `--quiet`	Permette di ridurre la quantità di informazioni che vengono emesse. Di solito può essere utile quando si usa il programma attraverso Cron.

Opzione	Descrizione
`-z` `--compress`	Prima di trasmettere i dati, li comprime. Ciò permette di ridurre il traffico di rete durante il trasferimento dei dati.
`-I` `--ignore-times`	Normalmente, si considera che i file che hanno la stessa dimensione e la stessa data di modifica, siano identici. Con questa opzione, si fa in modo che tale presunzione non sia valida.
`-c` `--checksum`	Fa in modo che vengano confrontati tutti i file attraverso un codice di controllo prima di decidere se devono essere trasferiti o meno. L'uso di questa opzione implica un tempo di elaborazione più lungo, anche se garantisce una sicurezza maggiore nella determinazione delle differenze esistenti tra l'origine e la destinazione.
`-a` `--archive`	Questa opzione rappresenta in pratica l'equivalente di '**`-rlptgoD`**' (ovvero la sequenza delle opzioni '**`--recursive`**', '**`--links`**', '**`--perms`**', '**`--time`**', '**`--group`**', '**`--owner`**', '**`--devices`**'), allo scopo di duplicare fedelmente tutte le caratteristiche originali, discendendo ricorsivamente le directory di origine.
`-r` `--recursive`	Richiede la copia ricorsiva delle directory, cioè di tutte le sottodirectory.

Opzione	Descrizione
`-R` `--relative`	Fa in modo di replicare nella destinazione, aggiungendolo a questa, il percorso indicato nell'origine, il quale deve comunque essere relativo.
`-b` `--backup`	Fa in modo di salvare temporaneamente i file che verrebbero sovrascritti da un aggiornamento. Questi vengono rinominati, aggiungendo un'estensione che generalmente è rappresentata dalla tilde ('**~**'). Questa estensione può essere modificata attraverso l'opzione '**`--suffix`**'.
`--suffix=`***suffisso***	Permette di definire il suffisso da usare per le copie di sicurezza dei file che vengono sovrascritti.
`-u` `--update`	Con questa opzione, si evita l'aggiornamento di file che nella destinazione risultano avere una data di modifica più recente di quella dei file di origine corrispondenti.
`-l` `--links`	Fa in modo che i collegamenti simbolici vengano ricreati fedelmente, come nell'origine.
`-L` `--copy-links`	Fa in modo che i collegamenti simbolici nell'origine, si traducano nella destinazione nei file a cui questi puntano.
`-H` `--hard-links`	Richiede la riproduzione fedele dei collegamenti fisici. Perché ciò possa avvenire, occorre che questi collegamenti si riferiscano allo stesso gruppo di file di origine che viene indicato nella riga di comando.

Opzione	Descrizione
`-W` `--whole-file`	Rsync utilizza normalmente un metodo che gli permette di trasferire solo il necessario per aggiornare ogni file. Con questa opzione, si richiede espressamente che ogni file da aggiornare sia inviato per intero. Questo può essere utile quando si allineano dati contenuti nella stessa macchina e qualunque elaborazione aggiuntiva servirebbe solo a rallentare l'operazione.
`-p` `--perms`	Riproduce fedelmente i permessi.
`-o` `--owner`	Quando Rsync viene utilizzato con i privilegi dell'utente '**`root`**', permette di assegnare a ciò che viene copiato lo stesso utente proprietario che risulta nell'origine.
`-g` `--group`	Quando Rsync viene utilizzato con i privilegi dell'utente '**`root`**', permette di assegnare a ciò che viene copiato lo stesso gruppo proprietario che risulta nell'origine.
`--numeric-ids`	Fa in modo di mantenere gli stessi numeri ID, quando le altre opzioni richiedono la riproduzione della proprietà dell'utente ('**`-o`**') o del gruppo ('**`-g`**').
`-D` `--devices`	Quando Rsync viene utilizzato con i privilegi dell'utente '**`root`**', permette di copiare i file di dispositivo.

Opzione	Descrizione
`-t` `--times`	Fa in modo che venga riprodotta fedelmente la data di modifica dei file.
`--partial`	Durante il trasferimento dei file, nella destinazione Rsync scarica i dati in un file «nascosto» (in quanto inizia con un punto). Quando un trasferimento viene interrotto, l'ultimo file il cui trasferimento non è stato completato, viene cancellato. Con questa opzione, si fa in modo di non perdere i trasferimenti parziali, recuperandoli la volta successiva.
`--progress`	Fa in modo di mostrare l'avanzamento del trasferimento dei singoli file, in modo da poter conoscere la situazione anche in presenza di file di grandi dimensioni.
`-P`	È l'equivalente della somma di '**`--partial`**' e di '**`--progress`**'.
`-n` `--dry-run`	Si limita a simulare l'operazione, senza eseguire alcuna copia. È utile per verificare l'effetto di un comando prima di eseguirlo veramente.
`-x` `--one-file-system`	Permette di non superare il file system di partenza, nell'origine.

Opzione	Descrizione
`--delete`	Fa sì che vengano cancellati i file nella destinazione che non si trovano nell'origine. Come si può intuire, si tratta di un'opzione molto delicata, in quanto un piccolo errore nell'indicazione dei percorsi si può tradurre nella perdita involontaria di dati. È questa la situazione più indicata per utilizzare l'opzione '**`-n`**' in modo da verificare in anticipo l'effetto del comando. In alcune circostanze può essere utile anche l'opzione '**`--force`**'. Se Rsync incontra dei problemi di lettura, la funzione di cancellazione viene inibita, salvo mantenerla attiva con l'opzione '**`--ignore-errors`**'.
`--delete-after`	Con questa opzione, assieme a '**`--delete`**', si fa in modo che la cancellazione dei file che non sono più nell'origine, avvenga alla fine delle altre operazioni; diversamente, ciò avviene all'inizio.
`--force`	Con questa opzione si consente la cancellazione di directory che non sono vuote quando devono essere rimpiazzate da file normali o comunque da file che non sono directory. Perché questa opzione venga presa in considerazione è necessario usare anche '**`-r`**' ('**`--recursive`**').

Opzione	Descrizione
`--ignore-errors`	Con questa opzione, assieme a '**`--delete`**', si conferma la richiesta di cancellazione anche in presenza di errori di lettura e scrittura dei dati.
`--exclude=`***modello***	Permette di indicare un nome di file (o directory), o un modello contenente metacaratteri, riferito a nomi da escludere dalla copia. Il nome o il modello indicato, non deve contenere riferimenti a percorsi; inoltre è bene che sia protetto in modo che non venga espanso dalla shell usata per avviare il comando. È il caso di sottolineare che, se viene escluso il nome di una directory si impedisce un eventuale attraversamento ricorsivo del suo contenuto.
`--exclude-from=`***file***	Si comporta come l'opzione '**`--exclude`**', con la differenza che il suo argomento è il nome di un file locale contenente un elenco di esclusioni.
`--bwlimit=`***kilobyte_al_sec***	Fa sì che il trasferimento non avvenga a una velocità maggiore di quella indicata, espressa in migliaia di byte al secondo. Tuttavia questa opzione è efficace solo per i trasferimenti che avvengono attraverso la rete, mentre viene ignorata per le unità di memorizzazione locali.

Opzione	Descrizione
`--password-file=`***file***	Quando è richiesta una forma di autenticazione fornendo una parola d'ordine, si può usare questa opzione per indicare il nome di un file di testo che la contenga. In alternativa, si può inserire questa informazione nella variabile di ambiente ***RSYNC_PASSWORD***.
`--password-file=`***file***	Quando è richiesta una forma di autenticazione fornendo una parola d'ordine, si può usare questa opzione per indicare il nome di un file di testo che la contenga; il file non deve consentire l'accesso a utenti diversi dal proprietario. In alternativa, si può inserire questa informazione nella variabile di ambiente ***RSYNC_PASSWORD***.
`-e=`***comando*** `--rsh=`***comando***	Permette di specificare il comando (il programma) da utilizzare come shell per l'accesso remoto. Normalmente viene usata '**`rsh`**', ma in alternativa si potrebbe utilizzare '**`ssh`**', o altro se disponibile. L'uso di una shell alternativa per l'accesso remoto, può essere configurato utilizzando la variabile di ambiente ***RSYNC_RSH***.
`--rsync-path=`***percorso***	Permette di specificare il percorso assoluto necessario ad avviare '**`rsync`**' nell'elaboratore remoto. Ciò è utile quando il programma non è nel percorso degli eseguibili nell'utenza remota.

Opzione	Descrizione

`-C`
 	
`--cvs-exclude`
	Questa opzione permette di escludere una serie di file, usati tipicamente da CVS, RCS e anche in altre situazioni, che generalmente non conviene trasferire. Si tratta dei nomi e dei modelli seguenti: ‘`RCS`’, ‘`SCCS`’, ‘`CVS`’, ‘`CVS.adm`’, ‘`RCSLOG`’, ‘`cvslog.*`’, ‘`tags`’, ‘`TAGS`’, ‘`.make.state`’, ‘`.nse_depinfo`’, ‘`*~`’, ‘`.#*`’, ‘`,*`’, ‘`*.old`’, ‘`*.bak`’, ‘`*.BAK`’, ‘`*.orig`’, ‘`*.rej`’, ‘`.del-*`’, ‘`*.a`’, ‘`*.o`’, ‘`*.obj`’, ‘`*.so`’, ‘`*.Z`’, ‘`*.elc`’, ‘`*.ln`’, ‘`core`’.
	Inoltre, vengono esclusi anche i file elencati all’interno di ‘`~/.cvsignore`’, della variabile di ambiente ***CVSIGNORE*** e all’interno di ogni file ‘`.cvsignore`’, ma in questo ultimo caso, solo in riferimento al contenuto della directory in cui si trovano.

Segue la descrizione di alcuni esempi.

- `$` **`rsync -r /tmp/prove roggen.brot.dg:/tmp/prove`** [*Invio*]

  Copia la directory ‘`/tmp/prove/`’ del nodo locale, assieme a tutto il suo contenuto, nel nodo *roggen.brot.dg*, generando lì, la directory ‘`/tmp/prove/prove/`’ contenente tutto ciò che discende dall’origine.

Si osservi che questa copia non riproduce le informazioni data-orario dei file e delle directory (servirebbe l'opzione '**-t**'), pertanto, se dovesse essere ripetuto il comando, si otterrebbe nuovamente il trasferimento di tutti i file.

- `# rsync -a /tmp/prove roggen.brot.dg:/tmp/prove` [*Invio*]

  Copia la directory '`/tmp/prove/`' del nodo locale, assieme a tutto il suo contenuto, nel nodo *roggen.brot.dg*, generando lì, la directory '`/tmp/prove/prove/`' contenente tutto ciò che discende dall'origine. La copia viene fatta riproducendo il più possibile le caratteristiche originali, comprese informazioni data-orario dei file e delle directory, così che un utilizzo successivo dello stesso comando trasferirebbe solo quanto necessario ad aggiornare la copia.

- `# rsync -a /tmp/prove/ roggen.brot.dg:/tmp/prove` [*Invio*]

  Copia il contenuto della directory '`/tmp/prove/`' del nodo locale nel nodo *roggen.brot.dg*, nella directory '`/tmp/prove/`'. La copia viene fatta riproducendo il più possibile le caratteristiche originali e la ripetizione del comando in momenti successivi trasferisce solo il necessario.

- `$ rsync -R prove/mie/*.txt roggen.brot.dg:/home/tizio` [*Invio*]

  Copia i file che terminano per '`.txt`' della directory '`prove/mie/`', discendente da quella attuale, nella directory '`/home/tizio/prove/mie/`' del nodo *dinkel.brot.dg*.

Si osservi che questa copia non riproduce le informazioni data-orario dei file e delle directory (servirebbe l'opzione '**-t**'), pertanto, se dovesse essere ripetuto il comando, si otterrebbe nuovamente il trasferimento di tutti i file.

- # **rsync -a -z -v /tmp/prove/ roggen.brot.dg:/tmp/prove** [*Invio*]

  Copia il contenuto della directory '`/tmp/prove/`' del nodo locale nella stessa directory nel nodo *roggen.brot.dg*. La copia viene fatta riproducendo il più possibile le caratteristiche originali, trasferendo dati compressi e visualizzando le operazioni compiute.

- # **rsync -azv -e ssh /tmp/prove/ roggen.brot.dg:/tmp/prove** [*Invio*]

  Come nell'esempio precedente, ma utilizza '**ssh**' come shell per l'accesso remoto.

- # **rsync -rlptD -zv /tmp/prove/ tizio@roggen.brot.dg:/tmp/prove** [*Invio*]

  Come nell'esempio precedente, ma utilizza la shell predefinita per l'accesso remoto e accede come utente '**tizio**'. Per questo, non tenta di riprodurre la proprietà dei file (utente e gruppo proprietario).

- # **rsync -rlptD -zv --progress** ↩
  ↪ **/tmp/prove/ tizio@roggen.brot.dg:/tmp/prove** [*Invio*]

  Come nell'esempio precedente, aggiungendo informazioni sul trasferimento dei singoli file.

- # **rsync -rlptD -zv --progress** ↩
  ↪ **/tmp/prove/ tizio@roggen.brot.dg::prove** [*Invio*]

Questo esempio è simile a quello precedente, con la differenza che nella destinazione si fa riferimento al modulo '**prove**'. I moduli di Rsync vengono descritti nelle sezioni successive, in occasione della presentazione delle funzionalità di servente di Rsync.

- `# rsync -rlptD -zv --progress ↩`
  `↪ /tmp/prove/ ↩`
  `↪ rsync://tizio@roggen.brot.dg/prove` [*Invio*]

Esattamente come nell'esempio precedente, usando una notazione diversa per la destinazione.

- `# rsync -rlptD -zv --progress ↩`
  `↪ /tmp/prove/varie/ ↩`
  `↪ rsync://tizio@roggen.brot.dg/prove/varie` [*Invio*]

Come nell'esempio precedente, con la differenza che si intende allineare solo una sottodirectory, precisamente '`/tmp/prove/varie/`', con la sottodirectory corrispondente nel modulo '**prove**'.

- `$ rsync --recursive ↩`
  `↪ --compress ↩`
  `↪ --links ↩`
  `↪ --perms ↩`
  `↪ --times ↩`
  `↪ --partial ↩`
  `↪ --checksum ↩`
  `↪ --verbose ↩`
  `↪ --progress ↩`
  `↪ rsync://roggen.brot.dg/prove/varie/ ↩`
  `↪ /home/prove/varie` [*Invio*]

In questo caso si vuole aggiornare il contenuto della directory locale '`/home/prove/varie/`' con il contenuto della directory

'`varie/`' del modulo '**`prove`**' presso l'elaboratore *roggen.brot.dg* che offre un accesso Rsync anonimo.

Come si può osservare dalle opzioni, si fa in modo di avere informazioni abbastanza dettagliate sullo svolgimento dell'operazione, per la presenza di '**`--verbose`**' e di '**`--progress`**'; inoltre, viene richiesto espressamente di verificare sempre i file da trasferire con un codice di controllo (opzione '**`--checksum`**') e di conservare i trasferimenti parziali (in modo da ridurre il lavoro di un aggiornamento successivo, in caso di interruzione della comunicazione).

Si osservi che la presenza dell'opzione '**`--checksum`**' richiede un impiego maggiore di risorse da parte di entrambi gli elaboratori coinvolti nel trasferimento, cosa che si traduce in tempi di attesa più lunghi.

- `$` **`rsync rsync://roggen.brot.dg`** [*Invio*]

  Con questo comando ci si limita a interrogare il servente Rsync remoto sulla sua disponibilità di moduli. Si osservi però che alcuni o anche tutti i moduli possono risultare nascosti, cioè non visibili in questo elenco, in base alla configurazione del servente stesso.

36.12.5 Accesso attraverso autenticazione

Quando è richiesta l'autenticazione attraverso una parola d'ordine l'uso della variabile di ambiente ***RSYNC_PASSWORD*** può essere molto utile per automatizzare le operazioni di sincronizzazione dati attraverso Rsync.

Quello che si vede sotto, potrebbe essere uno script personale di un utente che deve aggiornare frequentemente il modulo '**prove**' nel nodo *roggen.brot.dg* (identificandosi come '**tizio**'). Quando il servente remoto richiede la parola d'ordine, il cliente locale '**rsync**' la legge direttamente dalla variabile ***RSYNC_PASSWORD***:

```
#!/bin/sh
RSYNC_PASSWORD=1234ciao
export RSYNC_PASSWORD
rsync -rlptD -zv /tmp/prove/ rsync://tizio@roggen.brot.dg/prove
```

In alternativa alla variabile di ambiente ***RSYNC_PASSWORD***, si può usare un file esterno, con permessi di accesso limitati, specificando l'opzione '**--password-file**', come nell'esempio seguente:

```
#!/bin/sh
touch ~/.rsync-password
chmod go-rwx ~/.rsync-password
echo "1234ciao" > ~/.rsync-password
rsync -rlptD -zv --password-file=~/.rsync-password \
    /tmp/prove/ rsync://tizio@roggen.brot.dg/prove
rm -f ~/.rsync-password
```

Naturalmente, se Rsync non ottiene la parola d'ordine in uno di questi modi, la chiede in modo interattivo all'utente.

36.12.6 Servente Rsync

Se si vuole utilizzare Rsync per trasferire dati tra elaboratori differenti, senza usare una shell remota, occorre attivare nell'elaboratore remoto un servente Rsync. Si tratta in pratica dello stesso programma '**rsync**', ma avviato con l'opzione '**--daemon**'.

Il servente Rsync può essere avviato in modo indipendente, in ascol-

to da solo sulla porta TCP 873, oppure sotto il controllo del supervisore dei servizi di rete. In questa modalità di funzionamento è necessario predisporre un file di configurazione: '`/etc/rsyncd.conf`'.

Nel caso si voglia avviare il servente Rsync in modo autonomo dal supervisore dei servizi di rete, basta un comando come quello seguente:

```
# rsync --daemon[Invio]
```

Se si vuole inserire Rsync nel controllo del supervisore dei servizi di rete (cosa di sicuro consigliabile), occorre intervenire nel file '`/etc/services`' per definire il nome del servizio:

```
rsync           873/tcp
```

Inoltre occorre agire nel file '`/etc/inetd.conf`' (nel caso specifico di Inetd) per annunciarlo al supervisore dei servizi di rete:

```
rsync stream tcp nowait root /usr/bin/rsync rsyncd --daemon
```

Rsync utilizzato come servente si avvale del file di configurazione '`/etc/rsyncd.conf`' per definire una o più directory che si vogliono rendere accessibili attraverso il protocollo di Rsync, come una sorta di servizio FTP. Come nel caso dell'FTP, è possibile offrire l'accesso a chiunque, in modo anonimo, oppure si può distinguere tra utenti definiti all'interno della gestione di Rsync. Questi utenti sono potenzialmente estranei all'amministrazione del sistema operativo in cui Rsync si trova a funzionare, per cui occorre aggiungere un file di utenti e parole d'ordine specifico.

Rsync definisce ***moduli*** le aree che mette a disposizione (in lettura o anche in scrittura a seconda della configurazione). Quando si vuole

accedere a un modulo di Rsync si utilizza una delle due notazioni seguenti:

```
[utente_rsync@]nodo::modulo[/percorso_successivo]
```

```
rsync://[utente_rsync@]nodo/modulo[/percorso_successivo]
```

Quando si accede a un modulo, il servente Rsync può eseguire un ***chroot()*** nella directory a cui questo fa riferimento, più o meno come accade con l'FTP anonimo. Per fare un esempio concreto, se il modulo '**`prova`**' fa riferimento alla directory '`/home/dati/ciao/`' nel nodo *dinkel.brot.dg*, l'indirizzo '`dinkel.brot.dg::prova/uno/mio`', oppure '`rsync://dinkel.brot.dg/prova/uno/mio`', fa riferimento al percorso '`/home/dati/ciao/uno/mio`' in quell'elaboratore.

Ogni riga del file di configurazione descrive un tipo di informazione. Le righe vuote, quelle bianche e ciò che è preceduto dal simbolo '**#**' viene ignorato. È ammessa la continuazione nella riga successiva utilizzando la barra obliqua inversa ('****') alla fine della riga.

I moduli vengono identificati da un nome racchiuso tra parentesi quadre e la loro indicazione occupa tutta una riga; le informazioni riferite a un modulo sono costituite da tutte le direttive che appaiono nelle righe seguenti, fino all'indicazione di un altro modulo. Le direttive che descrivono i moduli sono delle opzioni che definiscono dei parametri e sono in pratica degli assegnamenti di valori a questi parametri. Alcuni tipi di parametri possono essere collocati prima di qualunque dichiarazione di modulo e si tratta in questo caso di

opzioni globali che riguardano tutti i moduli (alcuni parametri possono apparire solo all'inizio e non all'interno della dichiarazione dei moduli).

Le opzioni globali sono quelle direttive (o parametri) che si collocano prima della dichiarazione dei moduli. Alcuni parametri possono essere collocati solo in questa posizione, mentre gli altri, le opzioni dei moduli, pur essendo stati preparati per la descrizione dei singoli moduli, possono essere usati all'inizio per definire un'impostazione generale. L'elenco seguente mostra solo l'uso di alcuni parametri delle opzioni globali.

Tabella 36.159. Alcune direttive globali.

Direttiva	Descrizione
`motd file =` ***file***	Se presente, indica un file all'interno del quale viene prelevato il testo da mostrare agli utenti quando si connettono (il «messaggio del giorno»).
`max connections =` ↩ ↪***n_massimo_connessioni_simultanee***	Come avviene nel protocollo FTP, anche con Rsync può essere importante porre un limite alle connessioni simultanee. Se non viene specificata questa opzione, oppure se si usa il valore zero, non si intende porre alcuna restrizione.

Direttiva	Descrizione
`log file =` ***file***	In generale, i messaggi generati da Rsync durante il funzionamento come demone, sono diretti al registro di sistema, ma con l'uso di questa direttiva si può generare un file autonomo.
`pid file =` ***file***	Questa direttiva fa sì che Rsync scriva il numero del proprio processo elaborativo (PID) nel file indicato.

Tabella 36.160. Alcune direttive dei moduli.

Opzione	Descrizione
`comment =` ***stringa_di_descrizione_del_modulo***	Questa opzione permette di fornire una descrizione che può essere letta dagli utenti che accedono. Il suo scopo è chiarire il contenuto o il senso di un modulo il cui nome potrebbe non essere sufficiente per questo. Non è necessario racchiudere tra apici doppi il testo della stringa.

Opzione	Descrizione
`list =` ***yes*** | ***no*** `list =` ***true*** | ***false***	Con questa direttiva si controlla la possibilità di mostrare l'esistenza del modulo quando viene interrogato l'elenco di quelli esistenti. In condizioni normali, questa funzionalità è attiva e si può impedire la lettura assegnando il valore '**`no`**' o '**`false`**'.
`path =` ***percorso_della_directory***	Questo parametro è obbligatorio per ogni modulo. La direttiva serve a definire la directory, nel file system dell'elaboratore presso cui è in funzione il servente Rsync, a cui il modulo fa riferimento. Normalmente, attraverso la direttiva '**`use chroot`**' si fa in modo che, quando si accede al modulo, Rsync esegua la funzione ***chroot()*** in modo che la directory corrispondente appaia come la radice del modulo stesso.

Opzione	Descrizione
`use chroot =` ***yes*** | ***no*** `use chroot =` ***true*** | ***false***	Questo parametro è molto importante e consente, se si attribuisce un valore affermativo, di accedere alla directory del modulo attraverso la funzione ***chroot()***. Tuttavia, questa funzionalità può essere attivata solo se Rsync viene avviato con i privilegi dell'utente '**`root`**'.

`read only = true | false`
 	
`read only = yes | no`
	Questa opzione permette di definire se il modulo debba essere accessibile solo in lettura oppure anche in scrittura. Se l'opzione non viene specificata, si intende che l'accesso debba essere consentito in sola lettura. Assegnando il valore booleano '**`false`**' (oppure '**`no`**') si ottiene di consentire anche la scrittura.

Opzione	Descrizione
`uid =` ***nome_utente*** | ***id_utente*** `gid =` ***nome_gruppo*** | ***id_gruppo***	Queste due opzioni permettono di definire l'utente e il gruppo per conto dei quali devono essere svolte le operazioni all'interno del modulo. In pratica, Rsync utilizza quella identità per leggere o scrivere all'interno del modulo; questo può essere un mezzo attraverso il quale controllare gli accessi all'interno della directory corrispondente.
`auth users =` ***utente_rsync*** [`,` ***utente_rsync***] …	Questa opzione permette di indicare un elenco di nomi di utenti di Rsync a cui è consentito di accedere al modulo. Senza questa opzione, si concede l'accesso a chiunque, mentre in tal modo si impone il riconoscimento in base a un file di utenti definito attraverso il parametro '**`secrets file`**'.

Opzione	Descrizione
`secrets file = ↩` `↪`***file_di_utenti_e_parole_d'ordine***	Questa opzione è obbligatoria se viene usato il parametro '**`auth users`**'. Serve a indicare il file all'interno del quale Rsync può trovare l'elenco degli utenti e delle parole d'ordine (in chiaro).

`strict modes = true|false`
 	
`strict modes = yes|no`
	Questa opzione permette di stabilire se il file indicato con la direttiva '**`secrets file`**' debba essere accessibile esclusivamente all'utente associato al processo elaborativo di Rsync (di solito corrisponde a '**`root`**'), oppure se può mancare questa accortezza. In generale, questa opzione è attiva, a indicare che il file deve essere protetto.

Opzione	Descrizione

`ignore nonreadable = true|false`
 	
`strict modes = yes|no`
	Questa opzione permette di accettare la presenza di file che non risultano leggibili al servente Rsync. In pratica, con questa opzione attiva, si fa in modo che i file non leggibili siano trattati come se non esistessero del tutto.

`transfer logging = true|false`
 	
`strict modes = yes|no`
	Questa opzione, che normalmente non risulta attiva, se viene abilitata consente di far annotare nel registro i file trasferiti.

Opzione	Descrizione
`timeout =` ***n_secondi***	Questa opzione consente di specificare una scadenza alle connessioni, indicando un numero che esprime una quantità di secondi. Normalmente non c'è alcuna scadenza, ma in questo modo un errore da parte di un programma cliente potrebbe lasciare aperta una connessione inesistente all'infinito. In generale, se non ci sono altri problemi, conviene lasciare un tempo ragionevolmente grande, di una o più ore.
`max connections =` ***n***	Questa opzione consente di limitare la quantità massima di connessioni simultanee complessive. In mancanza di questa direttiva, nessun limite viene posto.

Opzione	Descrizione
`lock file =` ***file***	Questa opzione consente di stabilire espressamente il file da usare per il controllo del numero massimo di connessioni. In mancanza di questa indicazione, si tratta di '`/var/run/rsyncd.lock`'.

Segue la descrizione di alcuni esempi.

- ```
  uid = nobody
  gid = nobody
  [xxx]
          path = /home/xxx
          comment = Esportazione della directory /home/xxx
  ```

  Questo esempio, simile ad altri descritti nella pagina di manuale *rsyncd.conf(5)*, rappresenta una configurazione minima allo scopo di definire il modulo '**`xxx`**' che consenta l'accesso in sola lettura alla directory '`/home/xxx/`' per qualunque utente. Si osservi in particolare l'uso dei parametri '**`uid`**' e '**`gid`**', all'inizio del file, in modo che Rsync utilizzi i privilegi dell'utente e del gruppo '**`nobody`**' per la lettura dei file.

- ```
  [xxx]
          path = /home/xxx
          comment = Esportazione della directory /home/xxx
          uid = nobody
          gid = nobody
  ```

Si tratta di una variante dell'esempio precedente, in cui i parametri '**uid**' e '**gid**' sono stati collocati all'interno del modulo. In questo caso, dal momento che non ci sono altri moduli, l'effetto è lo stesso.

- ```
  [pippo]
          comment = Applicativo PIPPO
          path = /opt/pippo
          read only = false
          uid = tizio
          gid = tizio
          auth users = caio, sempronio
          secrets file = /etc/rsyncd.secrets
  ```

L'esempio mostra la descrizione del modulo '**pippo**' all'interno di un file di configurazione che potrebbe contenerne anche altri. In pratica, gli utenti che Rsync identifica come '**caio**' e '**sempronio**', possono scrivere all'interno della directory '`/opt/pippo/`', generando eventualmente anche delle sottodirectory, utilizzando i privilegi dell'utente e del gruppo '**tizio**' (secondo quanto definito dal sistema operativo di quell'elaboratore). Il file delle parole d'ordine necessario a identificare gli utenti '**caio**' e '**sempronio**' è '`/etc/rsyncd.secrets`'.
  ```

```
pid file=/var/run/rsyncd.pid
use chroot = yes
read only = yes
list = yes
uid = rsync
gid = rsync
secrets file = /etc/rsyncd.secrets
strict modes = yes
ignore nonreadable = yes
transfer logging = yes
timeout = 10800

[a2dist]
    comment = a2 distribution
    max connections = 7
    path = /home/a2dist/distribution
    auth users = tizio, caio, sempronio
```

Questo è un esempio abbastanza completo. Nella parte iniziale, le direttive globali servono a: specificare il file da usare per annotare il numero del processo elaborativo (PID); richiedere che venga utilizzata la funzione ***chroot()*** all'inizio di ogni modulo; consentire un accesso in sola lettura; consentire la visualizzazione dell'elenco dei moduli disponibili; far funzionare il programma servente con i privilegi dell'utente e del gruppo '**rsync**' (ma all'avvio il programma deve avere i privilegi dell'utente '**root**' e con questi privilegi va poi a leggere il file contenenti le parole d'ordine); specificare quale sia il file contenente le parole d'ordine, verificando che questo non risulti accessibile ad altri utenti; ignorare i file che non risultano leggibili, come se non ci fossero; annotare il trasferimento di tutti i file nel registro; far scadere le connessioni che durano oltre tre ore.

Dopo le direttive globali appare un solo modulo, denominato '**a2dist**', nel quale si indica: una descrizione del modulo; il limite massimo di connessioni (sette); il percorso del modulo (la directory '`/home/a2dist/distribution/`'); gli utenti autorizzati ad accedere al modulo.

Bisogna osservare che l'opzione '**max connections**' definisce la quantità massima di connessioni simultanee, in senso complessivo, anche quando la si utilizza all'interno dei moduli. In questo senso, mancherebbe la possibilità di stabilire una quantità massima di accessi simultanei riferiti al modulo e non a tutto l'insieme. Tuttavia, per tenere traccia del numero di connessioni, si utilizza un file, definibile con l'opzione '**lock file**'; pertanto, per distinguere le connessioni massime, modulo per modulo, basta cambiare nome a questo file:

```
pid file=/var/run/rsyncd.pid
use chroot = yes
read only = yes
list = yes
uid = rsync
gid = rsync
secrets file = /etc/rsyncd.secrets
strict modes = yes
ignore nonreadable = yes
transfer logging = yes
timeout = 10800

[a2dist-tizio]
    comment = a2 distribution for tizio
    max connections = 1
    path = /home/a2dist/distribution
    auth users = tizio
```

```
    lock file = /var/run/rsyncd.lock.tizio

[a2dist-caio]
    comment = a2 distribution for caio
    max connections = 1
    path = /home/a2dist/distribution
    auth users = caio
    lock file = /var/run/rsyncd.lock.caio

[a2dist-sempronio]
    comment = a2 distribution for sempronio
    max connections = 1
    path = /home/a2dist/distribution
    auth users = sempronio
    lock file = /var/run/rsyncd.lock.sempronio
```

L'esempio mostra la suddivisione in tre moduli per l'accesso agli stessi dati, ma da parte di tre utenti differenti, ognuno dei quali ha la disponibilità di un solo accesso simultaneo.

Nasce la necessità di impedire che un utente possa accedere per più di una volta, simultaneamente, quando la sincronizzazione richiede tempi lunghi. Per esempio, se Tizio configura il proprio sistema Cron per eseguire la sincronizzazione una volta al giorno, ma ci vuole più di un giorno per aggiornare tutto, si rischia di riavviare una seconda sincronizzazione errata.

36.12.6.1 File degli utenti e delle parole d'ordine secondo Rsync

Quando si utilizza Rsync come servente e si richiede una forma di autenticazione agli utenti che accedono, è necessario predisporre un file di testo contenente dei record secondo la sintassi seguente:

```
nome_utente:parola_d'ordine_in_chiaro
```

Dal momento che normalmente il file viene letto da Rsync con i privilegi dell'utente '**root**', è sufficiente che questo file abbia il permesso di lettura per l'amministratore del sistema.

Rsync non stabilisce quale sia la collocazione e il nome di questo file; è il parametro '**secrets file**' del file di configurazione a definirlo volta per volta. In generale, nella documentazione originale si fa l'esempio del file '`/etc/rsyncd.secrets`'. L'esempio seguente mostra il caso degli utenti '**caio**' e '**sempronio**', a cui sono state abbinate rispettivamente le parole d'ordine '**tazza**' e '**ciao**'.

```
caio:tazza
sempronio:ciao
```

È bene ribadire che questo file non ha alcun nesso con il file '`/etc/passwd`' (né con '`/etc/shadow`'). Gli utenti di Rsync possono non essere stati registrati (nel modo consueto) nell'elaboratore presso cui accedono.

36.12.7 Tempi morti e scadenze

«

Rsync è un sistema molto sofisticato per la sincronizzazione dei dati, in grado di consentire anche l'esecuzione del lavoro a più riprese, persino su file singoli (opzione '**--partial**'), con il minimo traffico di rete possibile.

Questa parsimonia nella gestione delle risorse di rete ha però un effetto indesiderato, in quanto si possono creare dei tempi morti, anche lunghi, in cui la connessione TCP rimane aperta senza il passaggio di alcun pacchetto. Tale situazione si può verificare in modo particolare quando si trasmettono file di grandi dimensioni attraverso dei tentativi successivi, perché ogni volta i due elaboratori coinvolti devono ricalcolare i codici di controllo di questi, per stabilire se la porzione presente nella destinazione possa essere utilizzata o meno: durante questo calcolo il traffico della connessione rallenta fino a sospendersi.

Anche se la sospensione della comunicazione non dovrebbe portare conseguenze per la connessione, bisogna ricordare questo fatto quando si utilizza la direttiva '**timeout**' (o l'opzione '**--timeout**'), in modo da lasciare un tempo sufficiente allo svolgimento delle operazioni necessarie. Inoltre, anche senza imporre alcun limite, ci potrebbero essere dei componenti tra i due elaboratori che non sono al corrente dell'esigenza di avere delle pause molto lunghe nelle connessioni. Potrebbe trattarsi di un router-NAT che deve seguire tutte le comunicazioni per le quali si richiede la trasformazione degli indirizzi e delle porte, introducendo anche per questo un problema di «scadenza» delle connessioni, cosa che così si può manifestare con delle interruzioni inspiegabili della sincronizzazione dei dati attraverso

Rsync.

Quando l'uso appropriato della direttiva '**timeout**' o dell'opzione '**--timeout**' non porta a risolvere il problema, può essere necessario evitare l'uso dell'opzione '**--partial**'.

36.12.8 Problemi di ricezione

Durante l'allineamento di una copia di dati, con Rsync, attraverso la rete, può succedere, in circostanze particolari, che l'elaboratore ricevente si blocchi.[29] Si osservi la figura successiva:

```
# rsync -a 172.17.1.254:/ /mnt/sda2
```

Nella figura si vede che l'elaboratore «A», sta allineando una propria copia di «B», a partire dalla directory '`/mnt/sda2/`'. Supponendo che l'elaboratore «B» sia in grado di generare un traffico molto fitto, può succedere che «A» si blocchi. In questi casi, l'unico rimedio consiste nell'uso dell'opzione '**--bwlimit**', cercando di trovare il livello di traffico massimo che non produce inconvenienti.

36.13 Riferimenti

- Christopher Smith, *NFS-HOWTO*, *http://nfs.sourceforge.net/nfs-howto/index.html*
- Thorsten Kukuk, *The Linux NIS(YP)/NYS/NIS+ HOWTO*, *http://tldp.org/HOWTO/NIS-HOWTO/*

- J. Reynolds, J. Postel, *RFC 1700, Assigned numbers, BOOTP and DHCP parameters*, 1994, http://www.ietf.org/rfc/rfc1700.txt
- *NTP home*, http://www.ntp.org
- *pool.ntp.org: public ntp time server for everyone*, http://www.pool.ntp.org
- David L. Mills, *Public NTP Time Servers*, http://www.eecis.udel.edu/~mills/ntp/servers.html
- *NET-SNMP*, http://www.net-snmp.org
- Andrea Manzini, *SNMP: tutta la rete in punta di Management Protocol*, *Linux&C.*, maggio 2006, 52, pag. 15, http://www.oltrelinux.com/
- Andrea Manzini, *Estensione di SNMPd e uso di MRTG*, *Linux&C.*, giugno 2006, 53, pag. 35, http://www.oltrelinux.com/
- Tobi Oetiker, *The Multi Router Traffic Grapher*, http://oss.oetiker.ch/mrtg/

[1] **Inetd** UCB BSD

[2] **TCP wrapper** software libero con licenza speciale

[3] **Portmapper** UCB BSD + SUN RPC

[4] **RPCinfo** UCB BSD + SUN RPC

[5] **Linux NFS** GNU GPL

[6] **YP Server** GNU GPL

[7] **YP Bind-mt** GNU GPL

[8] **YP Tools** GNU GPL

[9] Se non serve, o non funziona, si ottiene al massimo una segnalazione di errore nel momento in cui si utilizza il file-make, senza altri effetti collaterali.

[10] Di solito, il protocollo DHCP si utilizza per IPv4, dal momento che IPv6 risolve già i problemi di assegnazione automatica degli indirizzi.

[11] Il problema dell'instradamento esplicito verso la rete 255.255.255.255 si pone solo per kernel Linux molto vecchi e in generale si deve evitare di intervenire così.

[12] **DHCP ISC** software libero con licenza speciale

[13] **netkit-rwho** UCB BSD

[14] **netkit-rusers** software libero con licenza speciale

[15] **Finger** UCB BSD

[16] Non basta preoccuparsi di non attivare un servizio pericoloso: occorre verificare che non sia già presente in modo predefinito!

[17] **netkit-rsh** UCB BSD

[18] Si deve fare attenzione al fatto che tra il nome del nodo e il nome dell'utente, ci deve essere uno spazio.

[19] Per quanto riguarda le limitazioni all'accesso dell'utente '**`root`**', si tenga presente che potrebbe essere stato impedito l'accesso da un elaboratore remoto a causa della configurazione del file '`/etc/securetty`'.

[20] **Telnet** UCB BSD

[21] Un cliente TELNET è in grado di utilizzare soltanto il protocollo TCP. I servizi che si basano sul TCP utilizzano un proprio protocollo

di livello superiore ed è questo ciò a cui si fa riferimento.

[22] **netkit-tftp** UCB BSD

[23] **NTP** software libero con licenza speciale

[24] **NET SNMP** BSD

[25] **NET SNMP** BSD

[26] **NET SNMP** BSD

[27] **MRTG** GNU GPL

[28] **Rsync** GNU GPL

[29] Il problema si è manifestato su un elaboratore avviato con il file system principale innestato attraverso la rete (protocollo NFS), mentre con un file system locale ciò non accadrebbe. Pertanto, non si tratta di una questione legata specificatamente a Rsync, ma che comunque si può presentare con il suo utilizzo; per cui, in mancanza d'altro, si può rimediare abbassando la «velocità» con cui Rsync esegue la copia dei dati.