

## Malfunzionamenti della rete

### Introduzione

Lo scopo di questa sezione è quello di fornire strumenti di analisi per isolare le cause più comuni dei malfunzionamenti della rete. Si definiranno semplici procedure che occorrerà seguire per individuare e risolvere i più frequenti malfunzionamenti che si possono riscontrare in una rete di calcolatori. Spesso occorre verificare preliminarmente che il problema sussista effettivamente. Infatti capita non di rado che un utente associ alla non possibile fruizione di un servizio di rete problemi di connettività. Tipiche segnalazioni da parte dell'utenza sono per esempio: non riesco a scaricare la posta elettronica, non riesco a stampare, non riesco a visualizzare un sito Web,... In realtà se, per esempio, l'utente non riesce a leggere la posta elettronica, ma riesce a navigare con il suo Web browser, è molto probabile che ci sia solamente un problema di errata configurazione del suo programma per la lettura della posta elettronica piuttosto che si stia manifestando la momentanea indisponibilità del server email. Nel caso in cui invece più servizi di rete contemporaneamente non siano fruibili, allora è possibile che si tratti di un reale problema di rete.

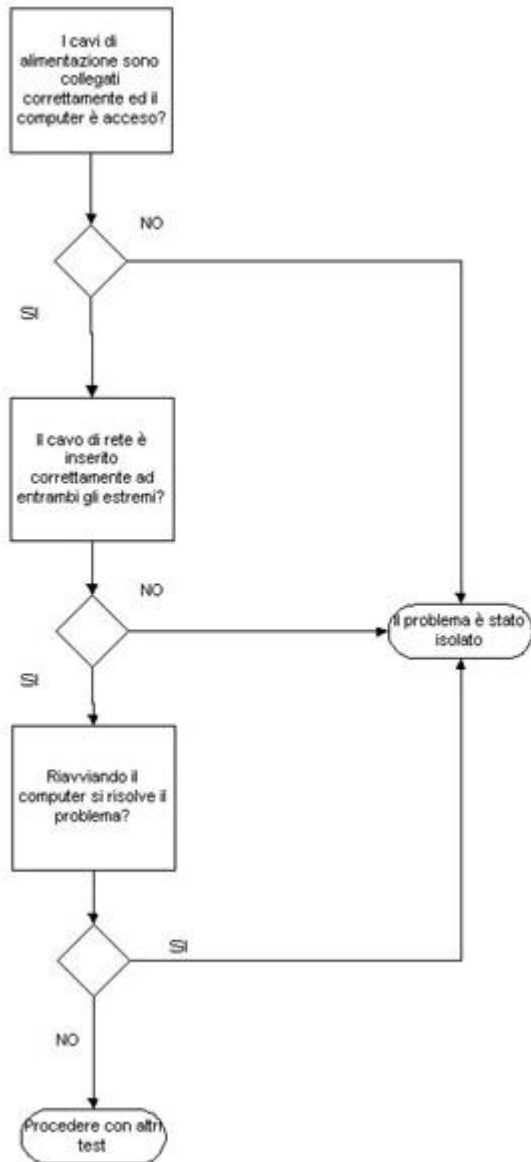
### Controllo fisico

Una volta accertato che si tratti di un problema di rete, occorre effettuare alcune verifiche che possono risultare ovvie, ma che spesso possono portare alla risoluzione:

- **Controllare l'alimentazione:** verificare che tutti i cavi di alimentazione siano collegati alle prese della rete elettrica e che il computer sia stato acceso.
- **Controllare la connettività:** verificare che il cavo di rete sia connesso saldamente alla **scheda di rete** ed alla presa a muro. Se il cavo connesso alla scheda di rete è di tipo **twisted pair** (rete **10 Base T** e **100 Base TX**), per esempio, estrarlo e reinserirlo fino a sentire il tipico click che si ha quando raggiunge la corretta posizione. Occorre fare attenzione che si stia usando un vero cavo di rete e non uno telefonico che è simile, ma ha connettori più piccoli (**RJ45** è il codice che identifica il primo contro **RJ11** che identifica il secondo).
- **Riavviare il computer:** provare a riavviare il computer, può darsi che reinizializzando il Sistema Operativo (SO) e la scheda di rete (*Network Interface Card*, NIC) il problema si risolva.

La sequenza di operazioni da seguire in questa fase preliminare è riassunta nel successivo diagramma di flusso.

Se, una volta eseguite queste verifiche, il problema non si risolve allora occorre procedere con altri test più dettagliati che vadano ad isolare l'ambito in cui questo risiede.



### Scambio di componenti di rete

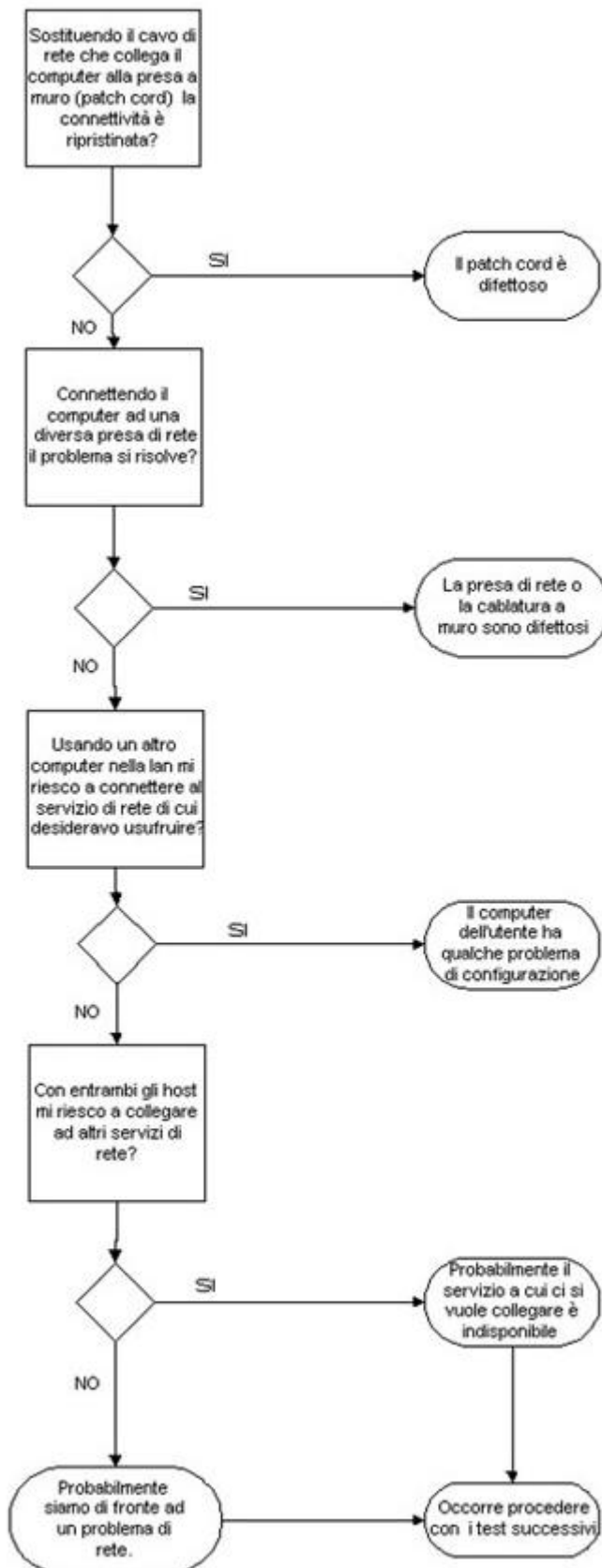
Spesso sulla scheda di rete è presente un **LED** illuminato; per verificare la stabilità connettività con un apparato di rete, come un **hub** od uno **switch**, occorre controllare lo stato di tale LED: se è spento allora sicuramente c'è un problema di connettività, mentre se è acceso non si può escludere ulteriori problemi, ma la connettività è fisicamente stabilita. Nel caso di **LED** spento occorre procedere con le successive operazioni necessarie ad isolare il problema:

- **provare a sostituire il cavo che connette la scheda di rete del computer alla presa a muro:** se a questo punto il LED si accende ed il computer riacquista tutte le funzionalità nell'uso della rete, significa che il problema era dovuto al cavo (*patch cord*) difettoso; se invece il LED non si accende ed è presente un'altra presa di rete vicina alla prima, allora si può passare alla fase successiva;
- **collegare il computer ad un'altra presa di rete:** se la connettività di rete è in questo caso presente, il problema è legato a difetti della prima presa di rete o della cablatura che la collega all'apparato di rete corrispondente; mentre se la connettività non è stabilita, il problema potrebbe risiedere nell'*host* stesso oppure potremmo essere di fronte effettivamente ad un malfunzionamento della rete. Occorre quindi procedere con ulteriori verifiche;
- **Usare un altro computer all'interno della LAN:** se questo computer si connette correttamente alla rete, allora probabilmente il problema risiede sull'*host* dell'utente e non sulla rete; se invece entrambi gli *host* non riescono a connettersi allo stesso servizio di rete, mentre

ciò non avviene con altri servizi di rete, allora il problema potrebbe risiedere sul server. Nel caso in cui entrambe le macchine non riescano ad accedere a tutti i servizi di rete, probabilmente si tratta di un effettivo malfunzionamento della rete ed occorre procedere con i test successivi.

In questi casi occorre capire se il problema si trova sull'*host* dell'utente (ovvero dal lato client), sull'*host* che ospita il servizio (lato server) oppure se si sta manifestando un malfunzionamento legato al *Domain Name System* (DNS) o ad un punto intermedio del percorso di rete che connette i due *endpoint* della comunicazione (problema di connettività).

Le operazioni appena descritte si riassumono nel seguente diagramma di flusso.



### Verifica della connettività IP

Supponiamo di voler connetterci ad una *host* per usufruire di un servizio di rete (Web, mail, FTP, telnet, ...), usando il protocollo TCP/IP e riferendolo mediante il suo nome nel DNS.

**Per esempio, connettendoci ad una Uniform Resource Locator (URL) di un Web server** (per esempio <http://www.unibo.it>), nel caso di malfunzionamento, potremmo ottenere due tipi di messaggio di errore che ci possono dare informazioni diverse:

- Se otteniamo un messaggio del tipo Errore 404, pagina non trovata vuol dire che la rete funziona correttamente, ma vi possono essere eventualmente problemi sul server.
- Se otteniamo un messaggio di errore del tipo il server non esiste o non posso trovare il server allora siamo di fronte ad un possibile problema di rete.

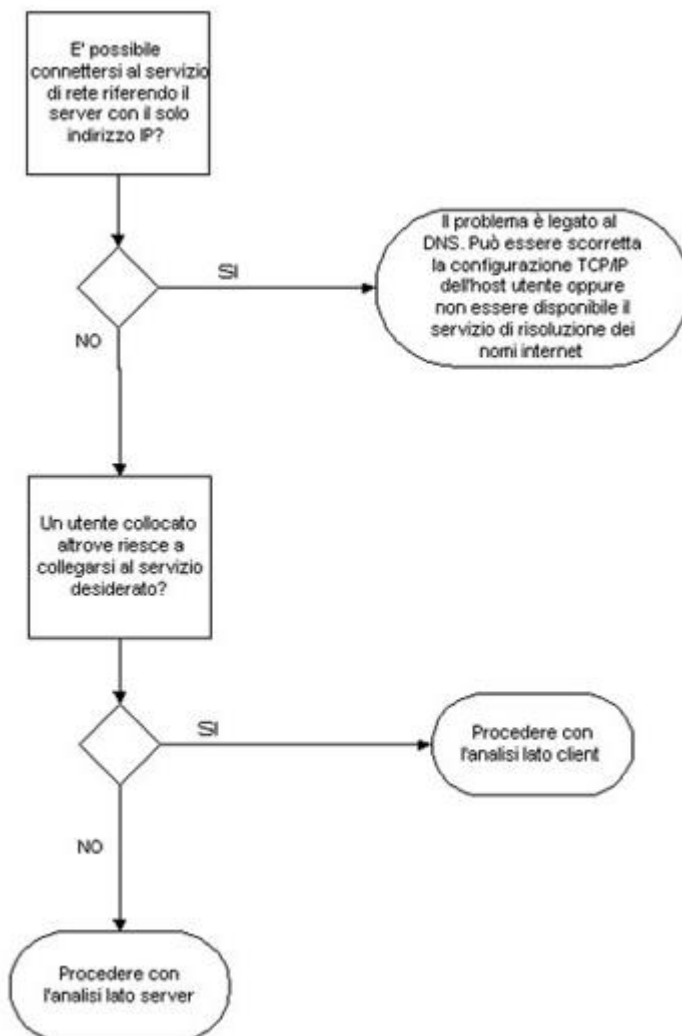
Se il server risulta raggiungibile mediante l'indicazione del solo indirizzo IP allora siamo di fronte ad un problema di DNS:

- Possono essere sbagliati i riferimenti ai **DNS server** nella configurazione di rete dell'*host* che manifesta il malfunzionamento;
- Può esserci un problema sui **DNS server** o possono non essere raggiungibili.

Se possibile, **chiedere ad un collaboratore di connettersi al server da una diversa locazione:**

- Se la connessione ha successo allora il problema si trova **lato client**;
- Se la connessione fallisce allora il problema è legato alla rete o si trova **lato server**.

Il diagramma di flusso che descrive questa procedura è riportato di seguito.



Analisi lato client

Come prima cosa occorre verificare la correttezza della configurazione di rete dell'*host* (quali indirizzo IP, *subnet mask*, *default gateway*) ed in particolare identificare quale sia l'indirizzo IP del *default gateway*.

Una volta accertato che tutto sia corretto, si può procedere a **lanciare il comando telnet e provare a collegarsi all'indirizzo IP del gateway**.

Se otteniamo in risposta il *prompt* di *login* del router allora probabilmente la nostra configurazione di rete è corretta ed il malfunzionamento è dovuto ad un problema di rete posto in un punto successivo al router.

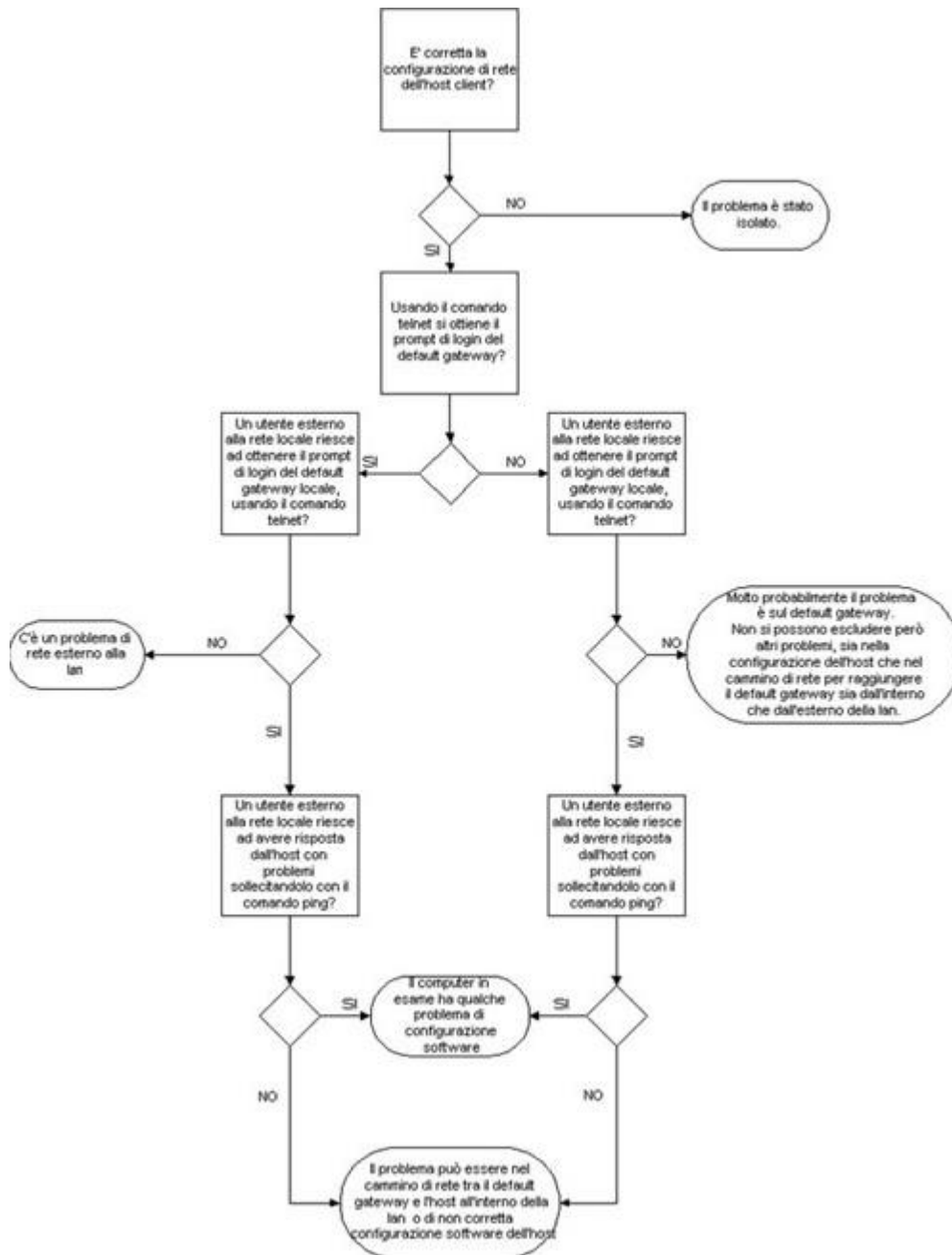
Se non riusciamo invece a connetterci al **default gateway**, allora potrebbe esserci un problema sul router o su un'apparecchiatura di rete intermedia.

In quest'ultimo caso si potrebbe chiedere ad un collaboratore, che si trovi in una diversa locazione nella rete, di **provare a collegarsi dall'esterno al router col comando telnet**.

Nel caso in cui l'operazione fallisca il problema può essere legato al router o al cammino di rete per raggiungerlo.

Se l'operazione ha successo si può provare a **sollecitare dall'esterno con un comando ping l'indirizzo IP della macchina che ha problemi**. Se questa risponde, allora il problema è sicuramente legato alla non corretta configurazione del software sull'*host* che si sta utilizzando, in caso contrario non si può escludere che sia un problema legato al cammino di rete tra il **default gateway** e l'*host* stesso.

Viene riportato nel successivo diagramma di flusso il percorso logico da seguire per portare a termine quest'ultima analisi.



### Analisi lato server (a livello applicazione)

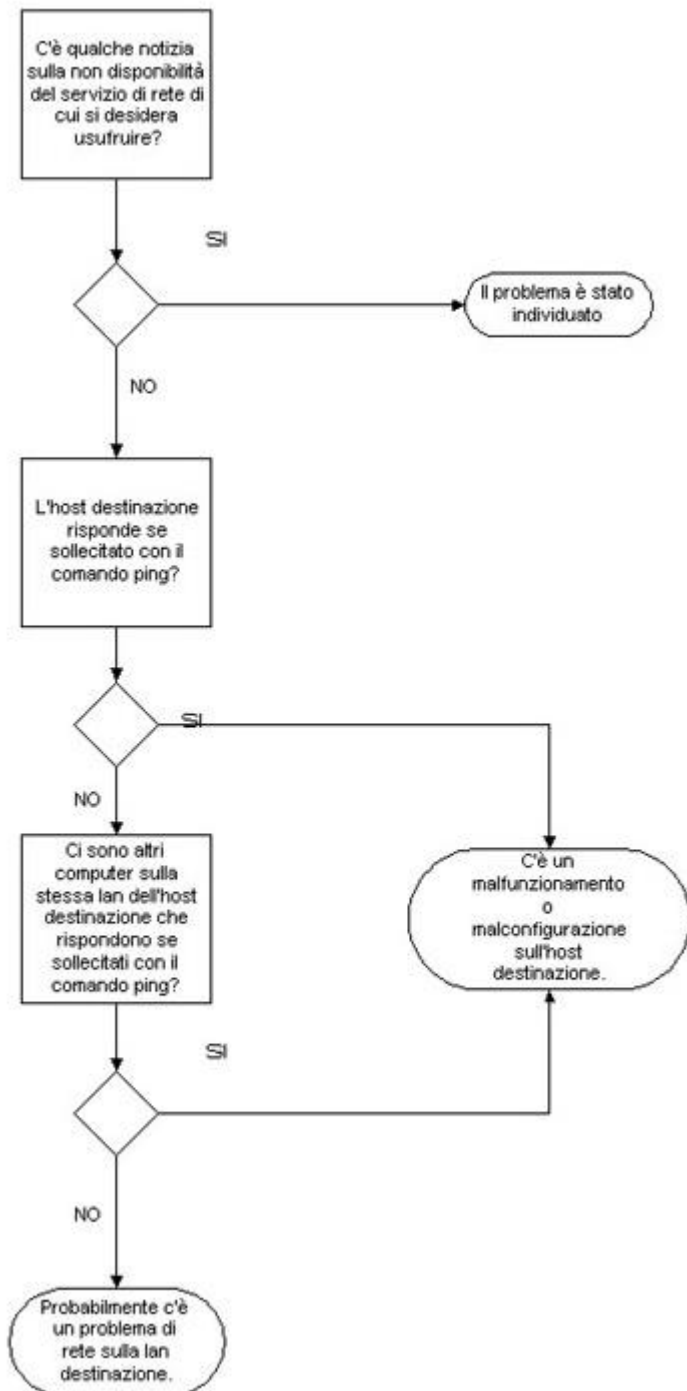
Nel caso si arrivi a questo punto dell'analisi, significa che, probabilmente, il problema risiede nella rete destinazione.

Come prima cosa occorrerebbe **informarsi se, per qualche motivo, il servizio di cui si desidera usufruire è momentaneamente indisponibile.**

In caso contrario sarebbe utile provare a sollecitare con un comando **ping** l'**indirizzo IP** della macchina destinazione. Se si ottengono risposte dall'*host* destinazione, allora vi è un malfunzionamento di quest'ultimo.

Se questo test non ha dato esito positivo allora è possibile cercare di sollecitare, mediante **un'applicazione per lo scanning di rete**, IP diversi da quelli della macchina destinazione. Se l'operazione ha successo (individuo *host* diversi da quello destinazione che rispondono al comando **ping** e che risiedono sempre sulla stessa LAN di quest'ultimo) allora il problema consiste in qualche malfunzionamento o non corretta configurazione della macchina destinazione, in caso contrario non si può escludere un problema nella rete *target*.

Il diagramma di flusso di quest'ultima analisi è il seguente.



Utility per la verifica del corretto funzionamento della rete: ICMP

Nelle procedure viste nei paragrafi precedenti si fa riferimento ad alcuni comandi, come *ping* e *telnet*, per potere verificare la raggiungibilità di *host* ed apparecchiature di rete.

Come ausilio alla gestione ed al monitoraggio della rete nella suite di protocolli TCP/IP usati dalla rete Internet è inserito il protocollo **ICMP** (*Internet Control Management Protocol*). Questo protocollo consente ai router presenti nel cammino di rete tra un *host* sorgente ed un *host* destinazione, di mandare al primo eventuali informazioni su malfunzionamenti di rete, in modo che possano prendere eventualmente provvedimenti correttivi. I pacchetti ICMP sono trattati allo stesso livello dei datagrammi IP e quindi seguono la filosofia *best effort* per la consegna, ovvero possono essere persi e possono eventualmente causare a loro volta congestione. L'unica differenza è che non possono generare, in caso di errori, a loro volta messaggi ICMP (non si generano cioè messaggi di errore su messaggi di errore).



Nell'*header* del pacchetto ICMP vi è un campo *TYPE* della lunghezza di 8 bit che identifica la tipologia del messaggio ICMP.

In particolare vi è una coppia di messaggi ICMP che permettono di verificare la raggiungibilità di un *host* da un altro:

### **TYPE MESSAGE**

0	<i>Echo Reply</i>
8	<i>Echo Request</i>

Inviando ad un *host* una richiesta **Echo Request** ed ottenendo da questo una risposta **Echo Reply** ne abbiamo verificato la raggiungibilità via rete. Un *utility* per inviare queste richieste è il comando **ping**, che è presente in praticamente tutti i sistemi operativi che abbiano funzionalità per il supporto della rete (Microsoft Windows 9x/ME/NT/2000/XP, UNIX, LINUX, e altri).

La sintassi del comando *ping* è la seguente:

```
ping [switch] [nome host destinazione| indirizzo IP host destinazione]
```

Come parametro si può esprimere il nome dell'*host* (normalmente il nome DNS, ma può essere anche un nome in stile **nbt** se ci troviamo su di una rete Microsoft) oppure direttamente il suo **indirizzo IP**. È possibile anche esprimere una serie di modificatori che permettono di variare il comportamento standard del comando.

Un esempio di uso del comando, se vogliamo verificare la raggiungibilità dell'*host* kaiser.alma.unibo.it, è

```
ping kaiser.alma.unibo.it
```

L'*output* che possiamo vedere su schermo, usandone la versione presente in Microsoft Windows XP Professional, è:



```

C:\Documents and Settings\iald>ping kaiser.alma.unibo.it

Pinging kaiser.alma.unibo.it [137.204.24.45] with 32 bytes of data:

Reply from 137.204.24.45: bytes=32 time<1ms TTL=61
Reply from 137.204.24.45: bytes=32 time<1ms TTL=61
Reply from 137.204.24.45: bytes=32 time<1ms TTL=61
Reply from 137.204.24.45: bytes=32 time<1ms TTL=61

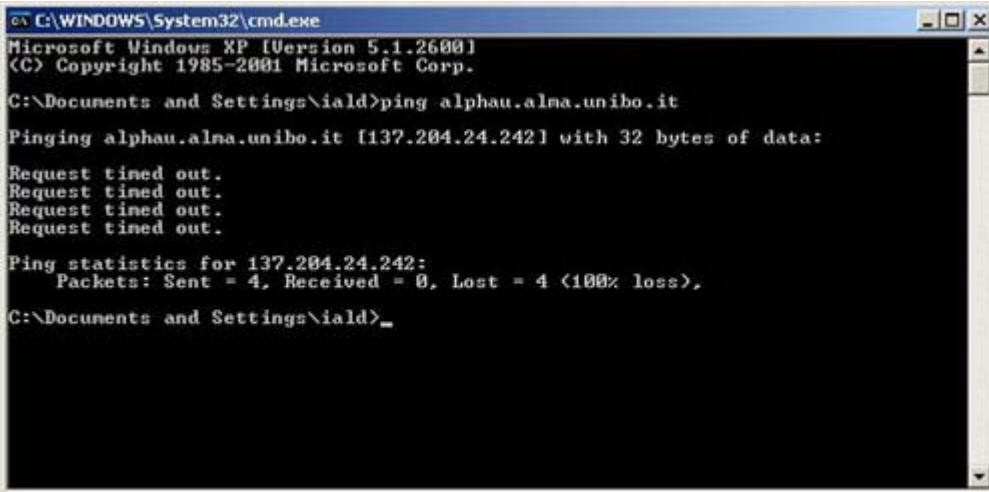
Ping statistics for 137.204.24.45:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\Documents and Settings\iald>_

```

In questo caso l'*host* è raggiungibile. Si può osservare, infatti, che sono state ottenute 4 risposte a 4 datagrammi di richiesta ed inoltre sono riportate ulteriori informazioni statistiche sul tempo di risposta, TTL (*Time To Live*), ecc..

Nel caso di *host* non raggiungibile avremmo avuto invece una schermata simile alla seguente:



```

C:\WINDOWS\System32\cmd.exe
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\iald>ping alpha.alna.unibo.it

Pinging alpha.alna.unibo.it [137.204.24.242] with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 137.204.24.242:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\Documents and Settings\iald>_

```

Come si può notare ogni richiesta ICMP *Echo Request* va in *timeout* in quanto non riceve una risposta ICMP *Echo Reply*.

Purtroppo non sempre è possibile fare uso di ICMP per la verifica dello stato di connettività della rete e della raggiungibilità degli *host*. Ad esempio, può capitare che in reti provviste di sistemi di protezione come firewall, il protocollo ICMP non sia permesso. Questo accade per evitare possibili attacchi di tipo DoS (**Denial of Service**) che mirano ad impedire l'utilizzo di un servizio da parte dell'utente, senza in realtà manifestare una vera e propria intrusione nei sistemi. Un tipico attacco DoS è il cosiddetto *Ping Flooding* (inondazione di *ping*) che mira a saturare la banda della rete vittima, impedendo quindi l'utilizzo delle sue funzionalità all'utente. Una protezione da questo tipo di attacco si realizza bloccando con un firewall il transito di datagrammi ICMP, ma si rinuncia alle funzionalità diagnostiche messe a disposizione dal protocollo. Sistemi di protezione più raffinati consentono l'uso di ICMP bloccandolo solo quando il numero di datagrammi in transito sembra elevato in modo anomalo. Per sapere se è possibile fare uso del *ping* per il test della rete occorrerebbe verificare, con gli amministratori della propria rete, le misure di protezione adottate.

Utility per la verifica del corretto funzionamento della rete: *tracert*

Un altro comando utile per verificare dove, all'interno del cammino di rete, si trova un problema di connettività, è *tracert* (**tracert** nei sistemi Microsoft).

La sintassi per questo comando è:

```
tracert [switch] [nome host destinazione| indirizzo IP host destinazione]
```

analoga a quella del comando *ping*.

Lanciando remotamente da una macchina UNIX, per esempio il seguente comando:

```
tracert www.csr.unibo.it
```

otteniamo il seguente *output*:

```

# traceroute www.csr.unibo.it
traceroute to web.csr.unibo.it (137.204.72.95), 30 hops max, 40 byte packets
 1  137.204.1.31 (137.204.1.31)  1 ms  1 ms  0 ms
 2  almr59 (137.204.2.15)  1 ms  1 ms  1 ms
 3  192.12.47.22 (192.12.47.22)  6 ms  6 ms  5 ms
 4  192.12.47.5 (192.12.47.5)  13 ms  10 ms  6 ms
 5  web.csr.unibo.it (137.204.72.95)  18 ms  21 ms  27 ms
#

```

Si può notare come siano evidenziati tutti i passaggi (**hop**) da apparati che si preoccupano dell'instradamento dei datagrammi e che sono presenti nel cammino di rete dall'*host* sorgente all'*host* destinazione.

Se l'*host* destinazione non è raggiungibile otterremo la lista relativa ai soli *hop* di apparati raggiungibili. In questo modo è possibile capire in quale punto del cammino di rete il problema si presenta.

Il funzionamento del comando *traceroute* si basa sull'invio all'indirizzo destinazione di datagrammi ICMP *Echo Request* con valore crescente del campo TTL (*Time To Live*) presente nell'*header*. Il campo TTL serve normalmente ad evitare che un datagramma circoli indefinitamente su Internet nel caso sfortunato che entri in un percorso di instradamento circolare (si può verificare questa eventualità quando c'è un malfunzionamento di qualche apparato di rete). Ad ogni passaggio di router, il valore di questo campo viene decrementato di uno. Nel caso in cui il valore raggiunga lo zero, il router che in quel momento ha in consegna il datagramma manda un messaggio ICMP all'indirizzo sorgente indicando che il pacchetto è stato scartato in quanto il TTL è scaduto:

#### **TYPE MESSAGE**

11 *Time Exceeded*

Sfruttando questo meccanismo ed inviando in sequenza datagrammi ICMP *Echo Request* con TTL crescenti a partire dal valore uno, otterremo in risposta, dai router intermedi tra il nostro *host* sorgente e destinazione, messaggi ICMP *Time Exceeded*. Nel caso di raggiungibilità dell'*host* destinazione, il processo terminerà quando il TTL sarà impostato al giusto numero di *hop* necessario per percorrere tutto il cammino di rete (in risposta all'ultimo datagramma inviato si avrà un ICMP *Echo Reply*). In caso contrario il processo terminerà quando si raggiungerà il numero massimo di *hop* previsto (normalmente 30). L'*utility traceroute*, analizzando l'*header* di ciascun datagramma ICMP ottenuto in risposta, è in grado di identificare l'indirizzo IP del router che lo ha generato e, eventualmente, di effettuare una *query* al DNS server per associargli un nome, se esistente.

Utility per la verifica del corretto funzionamento della rete: telnet

Un'altra *utility* per verificare la connettività di rete, di cui si è fatto cenno precedentemente, è il comando **telnet**.

Telnet è un'applicazione che ha funzionalità di emulatore di terminale remoto, cioè crea localmente una *shell* di comandi che in realtà sono eseguiti sull'*host* remoto a cui ci si è collegati. Viene stabilita una connessione TCP con il server (*host* a cui ci si collega) ed il terminale sull'*host* locale fa le veci di un terminale del sistema remoto.

Nell'esempio precedente, è usata questa applicazione per lanciare l'*utility traceroute* su un *host*

UNIX remoto.

La sintassi del comando telnet, che si può trovare praticamente su qualunque sistema operativo, è la seguente:

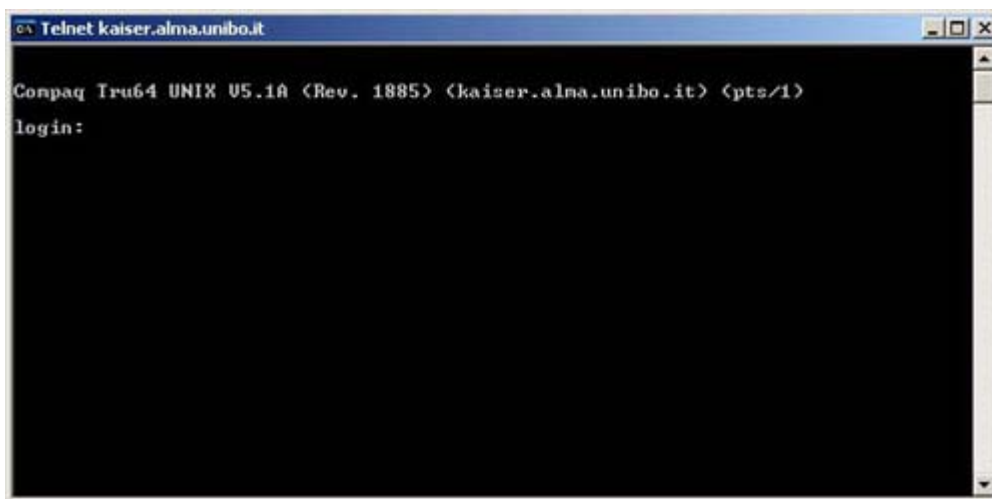
```
telnet [nome host destinazione| indirizzo IP host destinazione] [numero porta TCP]
```

Come si vede è possibile specificare il server mediante il suo nome o **indirizzo IP**. È possibile anche specificare una porta TCP a cui è associato il servizio al quale ci si vuole collegare. Se quest'ultimo parametro è omesso, la porta a cui ci si collega è la 23/TCP, che è il *default* per il server di emulazione di terminale remoto.

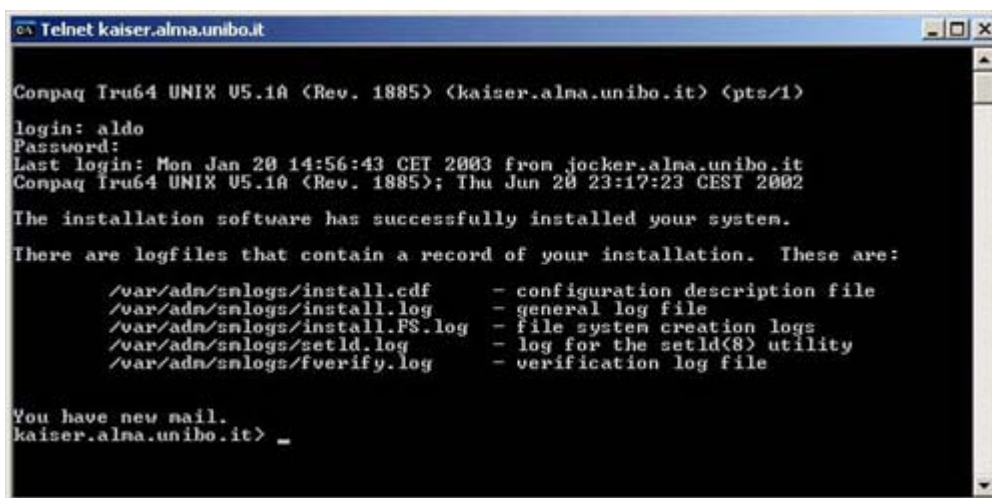
Volendo collegarci, per esempio, all'*host* UNIX kaiser.alma.unibo.it dovremmo digitare il comando

```
telnet kaiser.alma.unibo.it
```

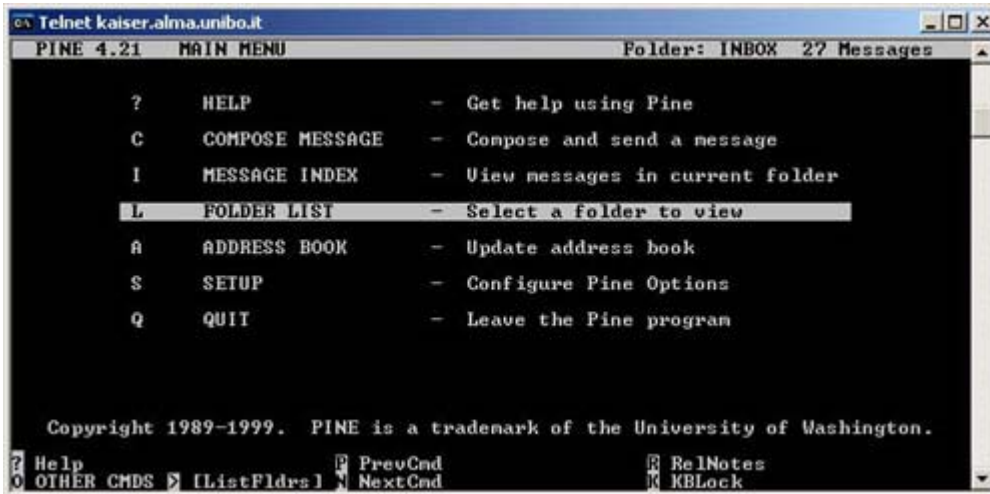
ottenendo come *output* un *prompt* di login:



Inserendo *username* e *password* appropriati avremo a disposizione una *shell* dove potere inserire comandi, come se avessimo acceduto fisicamente alla console dell'*host* remoto:

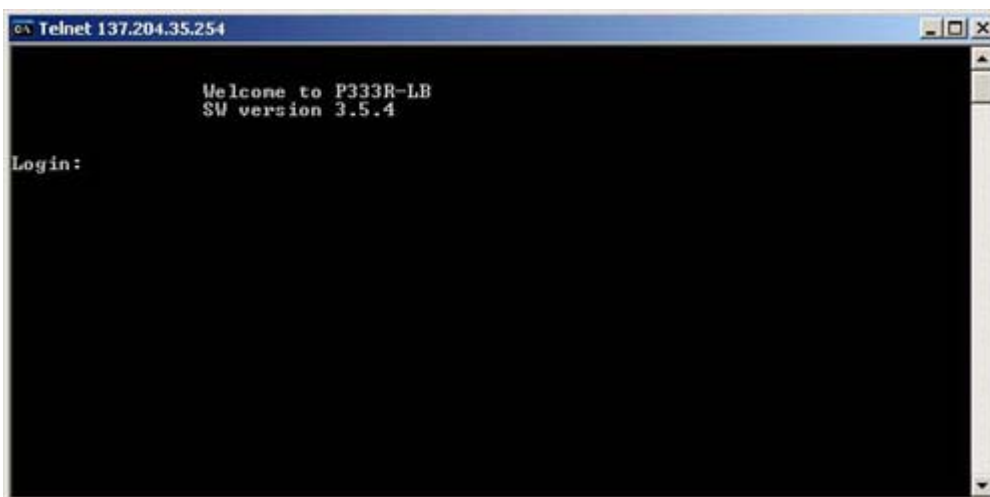


e quindi potremmo lanciare, per esempio, un programma per la lettura della posta elettronica a terminale:



L'*utility* telnet era stata citata, tra le altre cose, per valutare la possibilità di collegarsi al proprio *default gateway*.

In questo caso, se tutto funziona correttamente, si ottiene un *prompt* di *login* come per una macchina UNIX, ad esempio:

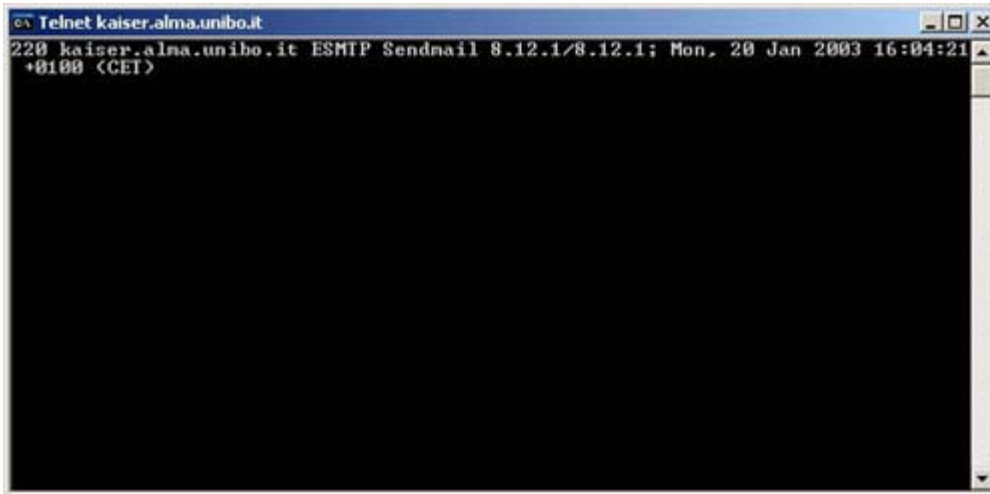


Abbiamo visto che è possibile specificare anche la porta TCP a cui l'*utility* telnet deve collegarsi. Questo consente di verificare anche la disponibilità dei servizi di rete presenti sui server di nostro interesse.

Sapendo che il servizio smtp di un server di posta si trova alla porta 25/TCP potremmo verificarne la disponibilità digitando, per esempio:

```
telnet kaiser.alma.unibo.it 25
```

Si otterrà in risposta:



```
Telnet kaiser.alma.unibo.it
220 kaiser.alma.unibo.it ESMTP Sendmail 8.12.1/8.12.1; Mon, 20 Jan 2003 16:04:21
+0100 <CEI>
```

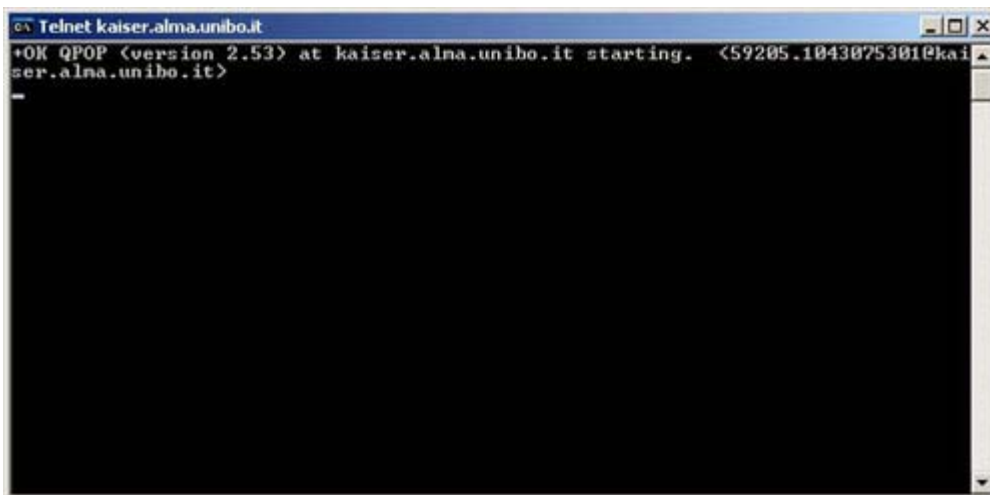
e cioè un *banner* che indica che il programma *sendmail* (il server di posta elettronica) è attivo ed in attesa di input.

Lo stesso si può fare se si desidera verificare la disponibilità del servizio POP3, che consente di scaricare la posta elettronica dal server al proprio *host*.

In questo caso si digiterà

```
telnet kaiser.alma.unibo.it 110
```

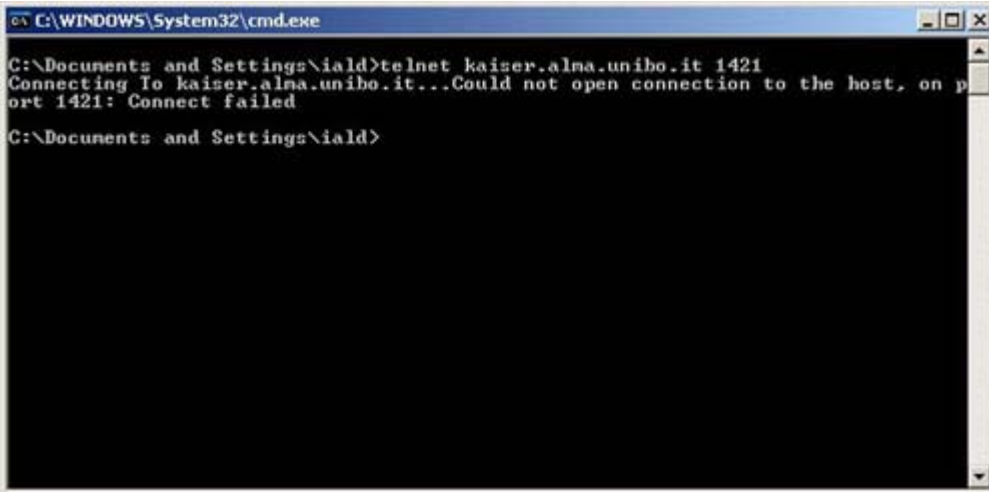
ottenendo in *output*:



```
Telnet kaiser.alma.unibo.it
+OK QPOP (version 2.53) at kaiser.alma.unibo.it starting. <59205.1043075301@kai
ser.alma.unibo.it>
```

cioè il *banner* del servizio POP3.

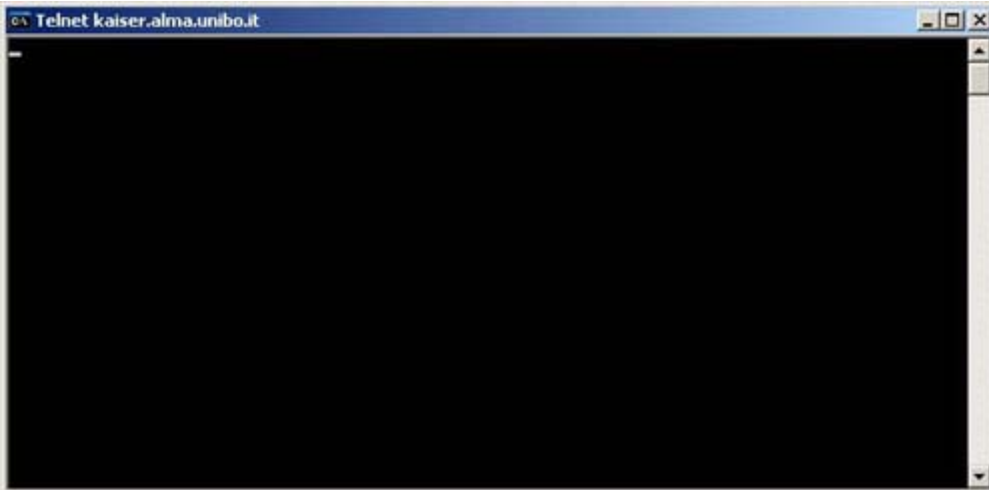
Nel caso in cui uno dei servizi non fosse stato attivo, avremmo ottenuto un *output* simile al seguente:



```
C:\WINDOWS\System32\cmd.exe
C:\Documents and Settings\iald>telnet kaiser.alma.unibo.it 1421
Connecting To kaiser.alma.unibo.it...Could not open connection to the host, on p
ort 1421: Connect failed
C:\Documents and Settings\iald>
```

Non è detto però che l'applicazione che ci interessa risponda sempre al telnet con un *banner*, anche nel caso in cui il servizio sia attivo.

Infatti, si potrebbe ottenere solo un *prompt* lampeggiante che resta in attesa di ulteriore input, come nella figura seguente:



```
Telnet kaiser.alma.unibo.it
_
```

Comunque, un *output* di questo tipo indica che il servizio è attivo e che la connessione TCP è stata stabilita.

Utility per la verifica del corretto funzionamento della rete: nslookup

Un'applicazione utile per interrogare direttamente ed in modo interattivo il DNS server è invece **nslookup**, presente sia su sistemi UNIX che su sistemi Microsoft. Può servire ad isolare problemi di rete legati alla risoluzione dei nomi.

Digitando il comando viene presentato un *prompt* a cui si possono sottoporre interrogazioni o comandi:



```

C:\WINDOWS\System32\cmd.exe - nslookup
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\iald>nslookup
Default Server:  kaiser.alma.unibo.it
Address:  137.204.24.45

>

```

Al *prompt* possiamo digitare un nome dns ottenendo in risposta l'indirizzo IP ad esso associato:

```

C:\WINDOWS\System32\cmd.exe - nslookup
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\iald>nslookup
Default Server:  kaiser.alma.unibo.it
Address:  137.204.24.45

> riddle.alma.unibo.it
Server:  kaiser.alma.unibo.it
Address:  137.204.24.45

Name:    riddle.alma.unibo.it
Address: 137.204.35.4

>

```

è possibile effettuare anche *query* per la risoluzione inversa, impostando opportunamente il tipo di record che si vuole cercare, ad esempio:

```

C:\WINDOWS\System32\cmd.exe - nslookup
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\iald>nslookup
Default Server:  kaiser.alma.unibo.it
Address:  137.204.24.45

> riddle.alma.unibo.it
Server:  kaiser.alma.unibo.it
Address:  137.204.24.45

Name:    riddle.alma.unibo.it
Address: 137.204.35.4

> set type=PTR
> 4.35.204.137.in-addr.arpa
Server:  kaiser.alma.unibo.it
Address:  137.204.24.45

4.35.204.137.in-addr.arpa      name = riddle.alma.unibo.it
35.204.137.IN-ADDR.ARPA      nameserver = kaiser.alma.unibo.it
35.204.137.IN-ADDR.ARPA      nameserver = almadns.unibo.it
kaiser.alma.unibo.it         internet address = 137.204.24.45
almadns.unibo.it             internet address = 137.204.1.15

>

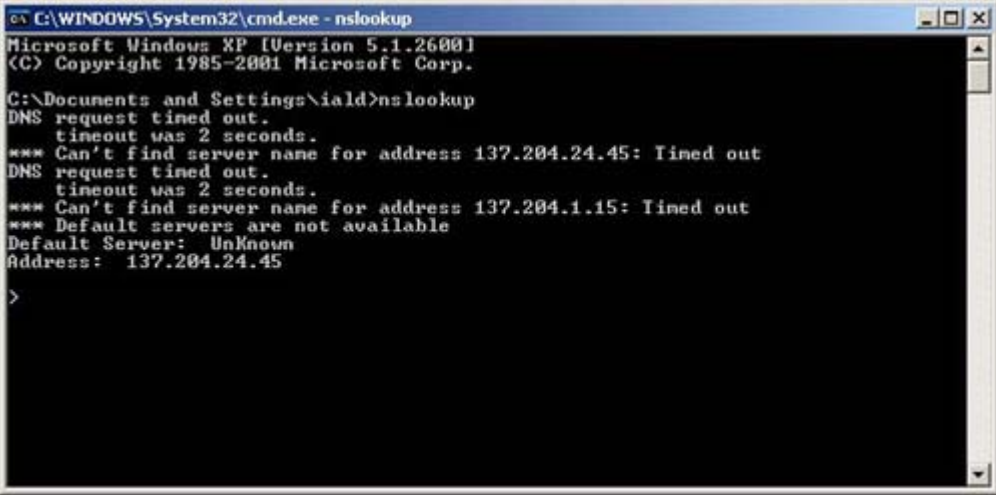
```

Come si può notare dalla figura, per potere sapere quale nome DNS è associato all'indirizzo IP 137.204.35.4 occorre impostare il tipo di record per la risoluzione inversa (*set type=PTR*) e poi usare nell'interrogazione il dominio in-addr.arpa facendolo precedere dall'indirizzo IP scritto con i 4 bytes in ordine inverso (4.35.204.137.in-addr.arpa) e ottenendo il nome riddle.alma.unibo.it che dalla



*query* diretta precedente era risultato essere associato all'indirizzo IP specificato.

È chiaro che se, durante la ricerca di un problema di rete che pensiamo essere legato al DNS, otteniamo come *output* del comando **nslookup** qualcosa di simile al seguente:



```

C:\WINDOWS\System32\cmd.exe - nslookup
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\iald>nslookup
DNS request timed out.
  timeout was 2 seconds.
*** Can't find server name for address 137.204.24.45: Timed out
DNS request timed out.
  timeout was 2 seconds.
*** Can't find server name for address 137.204.1.15: Timed out
*** Default servers are not available
Default Server: UnKnown
Address: 137.204.24.45

>

```

significa che sia il DNS server primario che quello secondario non sono, per qualche motivo, raggiungibili od il servizio di risoluzione dei nomi non è disponibile. Chiaramente in questa situazione non è possibile riferire gli *host* tramite il loro nome dns, ma solo tramite il loro **indirizzo IP** e ciò confermerà i nostri sospetti sulla correlazione dei malfunzionamenti con il DNS.

Utility per la verifica del corretto funzionamento della rete: netstat

Un comando utile per verificare se si sta manifestando un comportamento anomalo della rete è **netstat**. Questo comando, a seconda del modificatore specificato, può dare importanti informazioni e statistiche sul funzionamento della rete. In particolare il comando netstat -i su piattaforma UNIX e netstat -e su piattaforma Microsoft ci danno informazioni sui pacchetti transitati sulle interfacce di rete dell'*host*, con indicazione del numero di errori e di collisioni che si sono manifestati. Possiamo sicuramente affermare che, se il numero di collisioni supera il 10 % dei pacchetti transitati attraverso l'interfaccia, siamo sicuramente di fronte ad un comportamento anomalo ed occorre quindi procedere con successive analisi sul comportamento dell'*host* e delle apparecchiature di rete limitrofe.

Vengono riportati di seguito due esempi di *output* rispettivamente del comando netstat -e su un *host* con sistema operativo Microsoft Windows XP Professional e del comando netstat -i su un *host* basato su sistema operativo UNIX.



```

C:\WINDOWS\System32\cmd.exe

C:\Documents and Settings\iald>netstat -e
Interface Statistics

              Received              Sent
Bytes          822833                287696
Unicast packets    1753                1981
Non-unicast packets 2906                48
Discards          0
Errors            0
Unknown protocols 48

C:\Documents and Settings\iald>_

```

```

Telnet kaiser.alma.unibo.it
# netstat -i
Name Mtu Network Address Ipkts Ierrs Opkts Oerrs Coll
lo0 4096 <Link> Link#3 560158 0 560158 0 0
lo0 4096 loop localhost 560158 0 560158 0 0
slo0* 296 <Link> Link#2 0 0 0 0 0
tu0 1500 <Link> 0:0:f8:75:f2:7a 13888800 11743 25044584 0 0
tu0 1500 DLI none 13888800 11743 25044584 0 0
tu0 1500 137.204.24 kaiser 13888800 11743 25044584 0 0
tun0* 1280 <Link> Link#4 0 0 0 0 0
# -

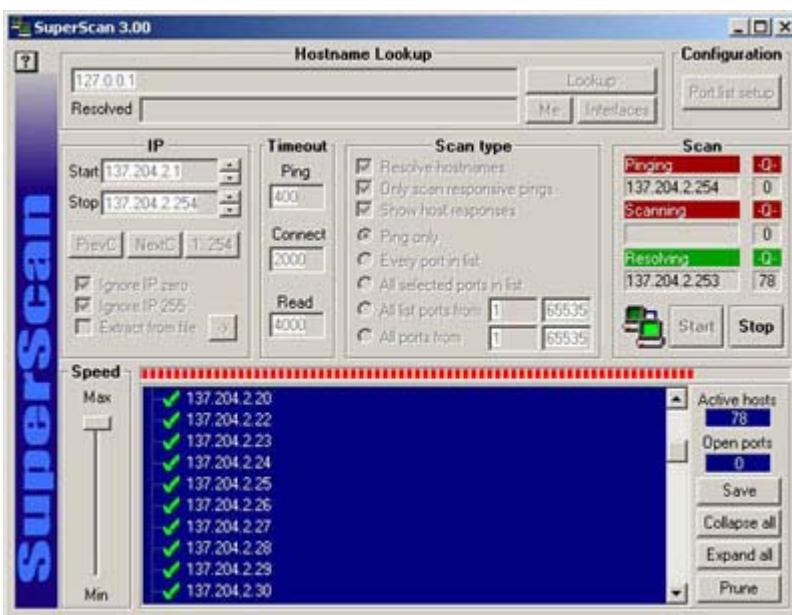
```

Come si può evincere dalle statistiche, in entrambi i casi il funzionamento della rete non presenta problemi rilevanti.

Il comando netstat permette di ottenere anche altre informazioni, quali le statistiche separate per protocollo, le tabelle di routing, le connessioni e le socket attive.

Utility per la verifica del corretto funzionamento della rete: scan IP

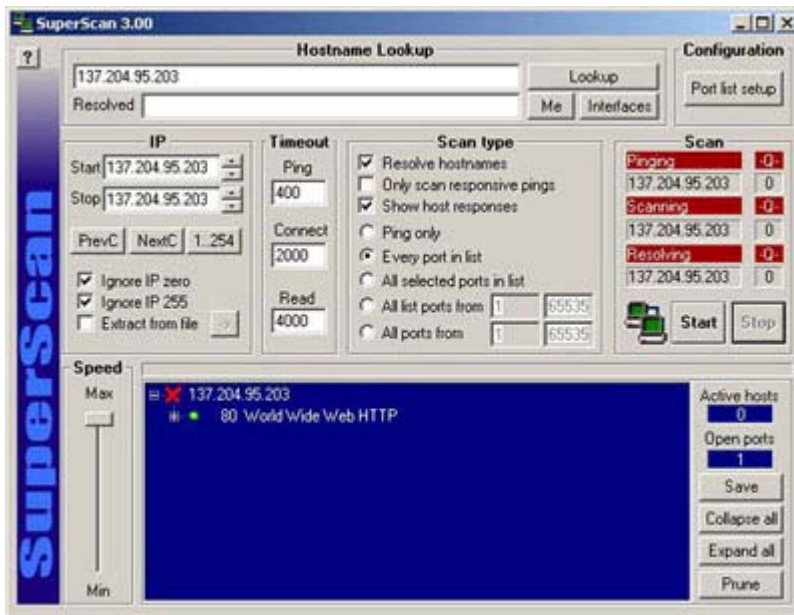
Nella sezione relativa alla procedura di analisi lato server si è fatto riferimento ad una generica applicazione di *scan* della rete per individuare *host* che rispondono al comando *ping*, in una determinata sottorete. Sul mercato si possono trovare diverse applicazioni di questo tipo, le quali, dato un *range* di indirizzi IP da analizzare, si preoccupano di effettuare iterativamente un comando *ping* su ciascuno di questi indirizzi. L'esempio riportato nella figura successiva mostra come viene testata la raggiungibilità degli *host* con IP *address* nel *range* 137.204.2.1 - 137.204.2.254.



Viene riportata come *output* la lista di indirizzi IP che rispondono al *ping*.

Le applicazioni di *scan* hanno normalmente funzionalità ulteriori, come l'analisi, in un *range* di porte specificato, della presenza di servizi attivi su un *host* o su insiemi di *host*.

Di seguito viene riportato l'*output* dello *scan* delle porte dell'*host* 137.204.95.203.



Come si può notare è attivo un servizio alla porta 80/TCP. Tale *host* è infatti un Web server. Si nota inoltre, dalla croce rossa, che, per motivi di sicurezza, l'*host* è stato configurato in modo tale da non rispondere alle sollecitazioni ICMP del comando *ping*.

Con quest'ultimo comando chiudiamo questa breve carrellata sulle semplici applicazioni utili nella ricerca e risoluzione dei malfunzionamenti della rete.

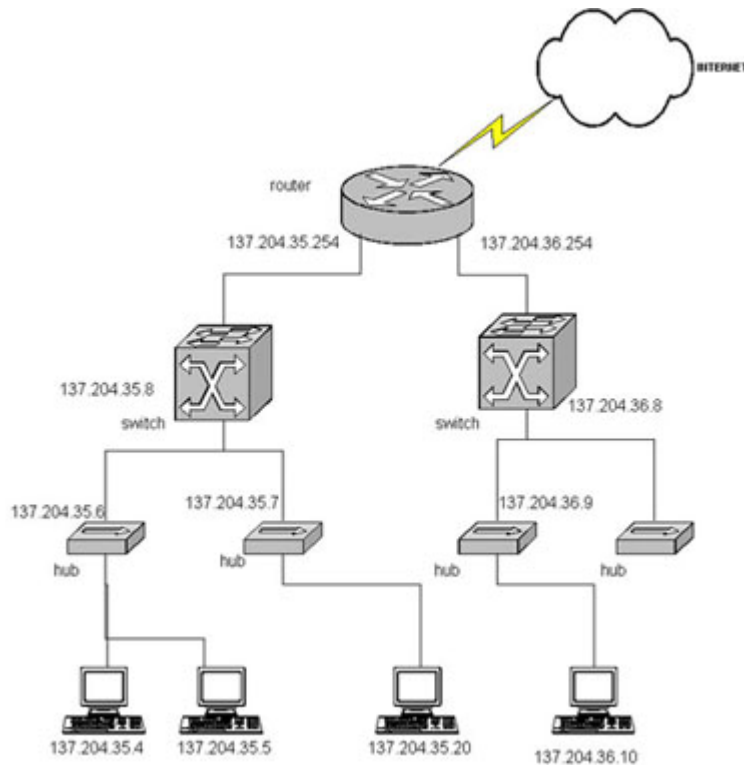
Ulteriori metodologie di analisi dei problemi

Quando si procede con l'analisi dei malfunzionamenti di rete, può essere utile tracciare a priori uno schema logico della topologia della propria rete di calcolatori. Avere a colpo d'occhio l'esatta disposizione delle apparecchiature che la compongono, permette di procedere in modo più efficace e mirato nell'individuazione della sorgente di un eventuale malfunzionamento ed alla sua conseguente eliminazione.

Per descrivere la metodologia che si può utilizzare in questi casi, come ulteriore livello di analisi da aggiungere a quelli precedentemente descritti, ipotizziamo di avere a che fare con una rete costituita da due *subnet* di classe C (137.204.35.0/24 e 137.204.36.0/24), aventi ciascuna una dorsale costituita da uno switch a cui sono collegati in cascata hub. Su questi ultimi vengono attestati gli *host*.

Ciascuno dei due switch è collegato ad una diversa interfaccia di un router, che costituisce il *default gateway* per le due sottoreti e che si preoccupa dell'instradamento dei datagrammi IP tra le due *subnet* ed il resto della rete Internet tramite una terza interfaccia.

La figura seguente rappresenta uno schema logico di tale rete.



Supponiamo che l'*host* con IP address 137.204.35.4 non riesca a connettersi ad un servizio di rete offerto dall'*host* con indirizzo 137.204.36.10. È possibile cercare di isolare il problema usando il comando *ping* visto precedentemente. L'idea è quella di sollecitare *host* all'inizio vicini e poi sempre più lontani, fino a che non si individua a quale livello nel cammino di rete si trova il problema. Inizialmente proviamo a sollecitare l'*host* 137.204.35.5, che si trova sullo stesso hub dell'*host* sorgente. Se non otteniamo risposta allora abbiamo già individuato che il problema risiede su questo primo hub. Per risolvere il problema potremmo provare a riavviarlo ed eventualmente ad analizzare la configurazione per riconoscere eventuali errori.

Se invece otteniamo risposta dall'*host* 137.204.35.5, passiamo a sollecitare l'*host* 137.204.35.20 che si trova su di un altro hub. Se non otteniamo risposta, il problema potrebbe risiedere sullo switch con IP address 137.204.35.8. Anche in questo caso possiamo provare a riavviarlo ed a verificarne la configurazione.

È a questo punto evidente quale sia lo schema di verifica da seguire. Procedendo secondo tale metodologia, si amplia progressivamente il cammino di rete percorso dal datagramma ICMP *Echo Request* inviato dal comando *ping*, introducendo una alla volta, nuove apparecchiature di rete, che si aggiungono a quelle che avevamo già verificato essere funzionanti. Si arriverà ad un punto, in questa procedura, in cui sarà possibile individuare qual'è l'apparato che presenta il malfunzionamento e risolverlo.

## Conclusioni

Questa trattazione introduttiva sulle problematiche legate ai malfunzionamenti della rete, mette in evidenza come sia necessario procedere in maniera strutturata all'isolamento del problema per poi passare alla sua risoluzione. Le metodologie esposte permettono di risolvere i problemi di rete che più frequentemente possono presentarsi in LAN non complesse. La loro applicazione ed una certa pratica consentiranno di acquisire dimestichezza e rapidità nell'individuazione e risoluzione di problematiche via via più complesse.

Sono disponibili approfondimenti relativi alle seguenti tematiche correlate:

- **Problematiche di rete in ambiente Microsoft Windows**
- **Protocollo SNMP**

I **referimenti bibliografici** consentono di svolgere autonomamente ulteriori attività di approfondimento.