Network Troubleshooting 101

Il titolo prettamente americano vuole rispondere al momento di panico capitato a tutti quando qualche cosa non funziona più: si è rotto il modem, o il mio provider è in crisi, o peggio ancora ho preso un Virus, o Windows è impazzita o ... ? Tutti, ma proprio tutti, possiamo fare delle minime verifiche di funzionamento delle nostre connessioni ad internet per cercare di capire dove è il problema prima di piangere e chiamare un esperto. Anche se le procedure sono comuni a qualunque macchina e sistema operativo, questa volta assumiamo di essere su di una macchina con OS Microsoft. Ci liberiamo immediatamente dall'interfaccia grafica, cliccando su **START** e poi **ESEGUI**, digitiamo `command` (o `cmd` nelle versioni più recenti), abbandoniamo il mouse e concentriamoci sulla tastiera.

C'è un motivo reale per fare questo: vogliamo utilizzare degli strumenti semplici il più possibile indipendenti dalle complicazioni della grafica e dei mille gadgets offerti dai programmoni che usiamo di solito. In questo modo speriamo di capire se il problema è locale (un programma od un Virus sul nostro computer) o remoto (di rete o di servizio del nostro provider). Nelle descrizioni seguenti indicheremo in **rosso** i comandi da digitare, ed in colore normale le risposte dei vari programmi. Riportiamo ovviamente solo il caso in cui il funzionamento sia normale, le anomalie sono immediate da rilevare.

1. Il primo passo è ottenere il nostro numero IP, basta digitare `ipconfig`[1]

```
ipconfig
Configurazione IP di Windows 98
0 - Scheda Ethernet :
      Indirizzo IP. . . . . . . . : 192.168.1.12
      Subnet Mask . . . . . . . . : 255.255.255.0
      Gateway predefinito . . . . : 192.168.1.1
```

ed ovviamente controllare che sia quello giusto. Il passo successivo è vedere dove la nostra macchina invia i pacchetti destinati ad altre macchine nella rete locale ed in internet. Il comando questa volta è `route print`[2]

1 Su piattaforme Unix/Linux il comando è `ifconfig` (alle volte è necessario indicare anche il path, ad esempio `/sbin/ifconfig`)

2 Su piattaforme Unix/Linux il comando è `route -n` (alle volte è necessario indicare anche il path, ad esempio `/sbin/route -n`)

```
route print
Route attive:
 Indirizzo rete  Maschera Ind.   gateway        Interfac.    Metric
 0.0.0.0         0.0.0.0         192.168.1.1    192.168.1.12    1
 127.0.0.0       255.0.0.0       127.0.0.1      127.0.0.1       1
 192.168.1.0     255.255.255.0   192.168.1.12   192.168.1.12    1
 192.168.1.12    255.255.255.255 127.0.0.1      127.0.0.1       1
 192.168.1.255   255.255.255.255 192.168.1.12   192.168.1.12    1
 224.0.0.0       224.0.0.0       192.168.1.12   192.168.1.12    1
 255.255.255.255 255.255.255.255 192.168.1.12   0.0.0.0         1
```

Il significato di questa tabella, a dir la verità un po' confusa, dovrebbe però essere chiaro: ad esempio per raggiungere internet devo passare da 192.168.1.1 che è il nostro gateway (firewall/router/modem ecc. per internet), invece 192.168.1.13 è locale e gli possiamo mandare i pacchetti direttamente.

2. Il punto successivo è verificare la connettività pura, per questo lo strumento indispensabile è `ping` che invia un pacchetto di testo (`icmp`) all'indirizzo IP indicato e ci dice se il pacchetto è stato ricevuto e quanto tempo ci ha messo a fare il tragitto di andata e ritorno.

```
ping 192.168.1.13
Esecuzione di Ping 192.168.1.13 con 32 byte di dati:
Risposta da 192.168.1.13: byte=32 durata=1ms TTL=255
Risposta da 192.168.1.13: byte=32 durata<10ms TTL=255
Risposta da 192.168.1.13: byte=32 durata<10ms TTL=255
Risposta da 192.168.1.13: byte=32 durata<10ms TTL=255
Statistiche Ping per 192.168.12.13:
    Pacchetti: Trasmessi = 4, Ricevuti = 4, Persi = 0 (0% persi),
Tempo approssimativo percorsi andata/ritorno in millisecondi:
    Minimo = 0ms, Massimo =  1ms, Medio =  0ms
```

Dobbiamo verificare (alcuni dei numeri IP utili possiamo ottenerli dal comando `route print` visto precedentemente):

- se siamo su di una LAN facciamo un `ping` all'indirizzo IP di un'altra macchina nella stessa LAN
- facciamo un `ping` all'indirizzo IP del nostro gateway verso internet
- facciamo un `ping` all'indirizzo IP del nostro server DNS
- facciamo un `ping` all'indirizzo IP di un gateway del nostro ISP (se lo conosciamo)
- facciamo un `ping` all'indirizzo IP di una macchina in internet (se lo conosciamo)
- facciamo un `ping` al nome di una macchina in internet, ad esempio www.miosito.it

Il terzo e l'ultimo ping ci permettono di verificare se la risoluzione dei nomi in numeri IP funziona.[3]

3. Se fin qui tutto funziona, vuol dire che abbiamo la connettività di base, il problema potrebbe

3 Se il server DNS non funziona, è possibile fare ben poco in internet!

però rimanere con alcuni servizi, ad esempio la posta elettronica o l'accesso ai siti Web. Possiamo fare delle verifiche anche per questi servizi direttamente. Per fare ciò usiamo il buon vecchio `telnet`. Per verificare se l'accesso Web funziona, scegliamo un sito che sappiamo essere attivo, e diamo i seguenti comandi:

```
telnet www.miosito.it 80

GET /index.html HTTP/1.1
Host: www.miosito.it

HTTP/1.1 200 OK
Date: Fri, 11 Jul 2003 12:38:31 GMT
Server: Apache/1.3.12 (Unix)
Transfer-Encoding: chunked
Content-Type: text/html

f70
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.0 Transitional//EN"
   "http://www.w3.org/TR/REC-html40/loose.dtd">
<HTML>
<HEAD>
      [ ... il resto della pagina in html ... ]
Connection closed by foreign host.
```

In questo caso `/index.html` è il nome della pagina che vogliamo vedere (spesso il carattere "/" è sufficiente). Da notare che dopo la riga con `Host` dobbiamo digitare una riga vuota, ovvero premere `Invio` due volte. Se ci colleghiamo ad internet attraverso un Proxy, bisogna fare il telnet verso il Proxy alla porta su cui esso è configurato, inoltre il comando `Host` non va dato (ma la riga vuota seguente si) e nel comando `GET` bisogna specificare tutto l'indirizzo della pagina richiesta, in questo esempio il comando sarebbe GET `http://www.miosito.it/index.html HTTP/1.1`.

4. Per quanto riguarda la posta elettronica, possiamo fare due verifiche. Recuperato il nome del server SMTP che usiamo per inviare la posta, facciamo prima un `ping` per vedere se è attivo, e poi proviamo a spedire a noi stessi un messaggio di prova:

```
telnet mio.smtp.server 25

220 mio.smtp.server ESMTP Postfix
EHLO mio.smtp.server
250-smtp.mio.server
250-PIPELINING
250-SIZE 10240000
250-VRFY
250-ETRN
250-XVERP
250 8BITMIME
MAIL FROM: mestesso@mioprovider.it
250 Ok
RCPT TO: mestesso@mioprovider.it
250 Ok
DATA
354 End data with <CR><LF>.<CR><LF>
test smtp by hand
.
250 Ok: queued as 4DB732798C
QUIT
221 Bye
Connection closed by foreign host.
```

In pratica abbiamo mandato da noi stessi a noi stessi un messaggio (senza titolo o mittente esplicito che volendo è facile aggiungere) il cui testo è *test smtp by hand*. Si finisce il testo del messaggio e lo si invia digitando una riga che contiene solo un punto, cioè "." e subito dopo Invio.

Andiamo ora a verificare se il messaggio è arrivato al nostro Provider. Assumiamo che il metodo di connessione al nostro Provider per scaricare la posta in arrivo sia tramite il protocollo POP3, il più comune. Facciamo un ping al server e se risponde proviamo a connetterci

```
telnet pop3.isp.it 110

+OK Server POP3 server ready
USER mio_username
+OK username accepted
PASS mia_password
+OK authentication successful
STAT
+OK 0 0
+OK 1 1217
QUIT
+OK session ended
Connection closed by foreign host.
```

Il comando `STAT` elenca lo stato della mailbox, quanti messaggi ci sono e quanto grandi ed è di solito sufficiente per verificare la funzionalità del servizio. In questo caso c'è solo un messaggio, quello che abbiamo appena mandato, di 1217 Bytes.

Andrea Pasquinucci
Consulente di Sicurezza Informatica
pasquinucci@ucci.it

Riferimenti Bibliografici:

[1] I riferimenti più utili sono gli standard di base di internet: RFC-2821 per smtp, RFC-1939 per pop3, RFC-792 per icmp, RFC-2616 e RFC-2817 per http.