

Laboratorio di Amministratore di Sistema

8. Ricerca e gestione dei guasti

[Cisco ITESS II - Chapter 13]

Università di Venezia – Facoltà di Informatica
feb-mag 2013 - [A. Memo](#)



ver 2.1

Troubleshooting the Operating System

13.1 identificazione e la localizzazione Sintomi e problemi

13.1.1 Problemi hardware

13.4 Risoluzione dei problemi di rete

13.4.1 Perdita di connettività

13.4.3 Utilizzo di programmi di utilità TCP / IP

Hardware Problems

Sebbene alcuni problemi sono dovuti ad una combinazione di fattori, la maggior parte può essere isolato in origine ad uno di questi:

- Hardware - Un componente di hardware del sistema è malfunzionamento, o atteso ma non presente.
- Kernel - Un bug o mancanza di funzionalità nel kernel del sistema a volte causa problemi di origine ambigua.
- Software applicativo - software applicativo livello utente o utilità di comando possono comportarsi in modo strano, o semplicemente crollare.
- Configurazione - Servizi di sistema o software applicativi può essere configurato in modo errato.
- Errore utente - Una delle fonti più frequenti di errore condizioni sono causati da utenti di computer che tentano di fare qualcosa nel modo sbagliato.

Hardware Problems

- Ogni sorta di condizione di errore può essere classificato in due modi, sia coerente o incoerente.
- Alcuni errori hardware saanno evidenti. Altri lascian tracce che il kernel rileva e registra.
- Assumendo che un errore non blocchi il sistema, la prova potrebbe essere lasciata nel file di registro

/ var / log / messages

con il messaggio precedente viene prefissata la parola OOOOPPS.

```
Aug 5 09:35:38 cisco-flerb xfs: ignoring font path element /usr/X11R6/lib/X11/fonts/cyrillic (unreadable)
Aug 5 09:35:38 cisco-flerb smb: smbd startup succeeded
Aug 5 09:35:38 cisco-flerb kernel: Oops: 0002 [#1]
Aug 5 09:35:38 cisco-flerb su(pam_unix)[1443]: session opened for user root by rtaibot(uid=500)
```

Using System Utilities and System Status Tools

- I sistemi operativi Linux forniscono vario sistema di utility e strumenti di stato del sistema:
 - setserial
 - lpq
 - ifconfig
 - percorso
- Le seguenti utilità torneranno informazioni su come il sistema o un file "dovrebbe" essere configurato.

Using System Utilities and System Status Tools

- L'utilità `setserial` fornisce informazioni e opzioni di set per le porte seriali del sistema.
- In genere le porte seriali sono `/dev/ttyS0` e `/dev/ttyS1`
- Per ottenere informazioni dettagliate su una particolare porta seriale:

`#setserial -a /dev/ttyS0`

The `setserial` Command

```
Password:
[root@cisco-flerb home]# setserial -a /dev/ttyS0
/dev/ttyS0, Line 0, UART: 16550A, Port: 0x03f8, IRQ: 4
      Baud_base: 115200, close_delay: 50, divisor: 0
      closing_wait: 3000
      Flags: spd_normal skip_test

[root@cisco-flerb home]#
```

Using System Utilities and System Status Tools

- Il comando `lpq` aiuta a risolvere i problemi di stampa.
- Il comando visualizzerà tutti i file in attesa di essere stampato.
- Se il lavoro di stampa che è stata presentata scompare dalla coda, allora c'è qualcosa di sbagliato con la coda di stampa

The `lpq` Command

```
[root@cisco-flerb rtalbot]# lpq
Printer: ph2-hp8100-1@cisco-flerb (dest ph2-hp8100-1@print-phoenix2.cisco.com)
Queue: no printable jobs in queue
Status: job 'cfA959cisco-flerb.cisco.com' removed at 14:29:38.971
no entries
[root@cisco-flerb rtalbot]#
```

Using System Utilities and System Status Tools

- Il comando ifconfig può essere immesso nella shell per riportare la configurazione di interfaccia di rete corrente del sistema.

```
[root@cisco-flerb home]# ifconfig
eth0      Link encap:Ethernet  HWaddr 00:10:B5:91:0F:F9
          inet addr:64.101.105.102  Bcast: 255.255.255.255  Mask:255.255.255.128
          UP BROADCAST NOTRAILERS RUNNING MTU:1500  Metric:1
          RX packets:16713 errors:0 dropped:0 overruns:0 frame:0
          TX packets:2140 errors:0 dropped:0 overruns:0 carrier:0
          collisions:137 txqueuelen:100
          RX bytes:2039255 (1.9 Mb)  TX bytes:1242702 (1.1 Mb)
          Interrupt:10 Base address:0x9400

lo        Link encap:Local Loopback
          inet addr:127.0.0.1 Mask:255.0.0.0
          UP LOOPBACK RUNNING MTU:16436 Metric:1
          RX packets:386 errors:0 dropped:0 overruns:0 frame:0
          TX packets:386 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:30622 (29.9 Kb)  TX bytes:30622 (29.9Kb)

[root@cisco-flerb home]#
```


Using System Utilities and System Status Tools

- Il comando route visualizza o imposta le informazioni sul instradamento del sistema, che utilizza per inviare informazioni a particolari indirizzi IP.

The route Command

```
[root@cisco-flerb home]# route
Kernel IP routing table
Destination    Gateway         Genmask         Flags   Metric  Ref    Use Iface
64.101.115.0   *               255.255.255.128 U        0      0      0 eth0
127.0.0.0      *               255.0.0.0      U        0      0      0 lo
default        hsrp-64-101-115 0.0.0.0        UG       0      0      0 eth0
[root@cisco-flerb home]#
```

destination network

gateway address
* = none set

netmask for the destination net
255.255.255.255 = host 0.0.0.0 = default

U = route is up
G = use gateway

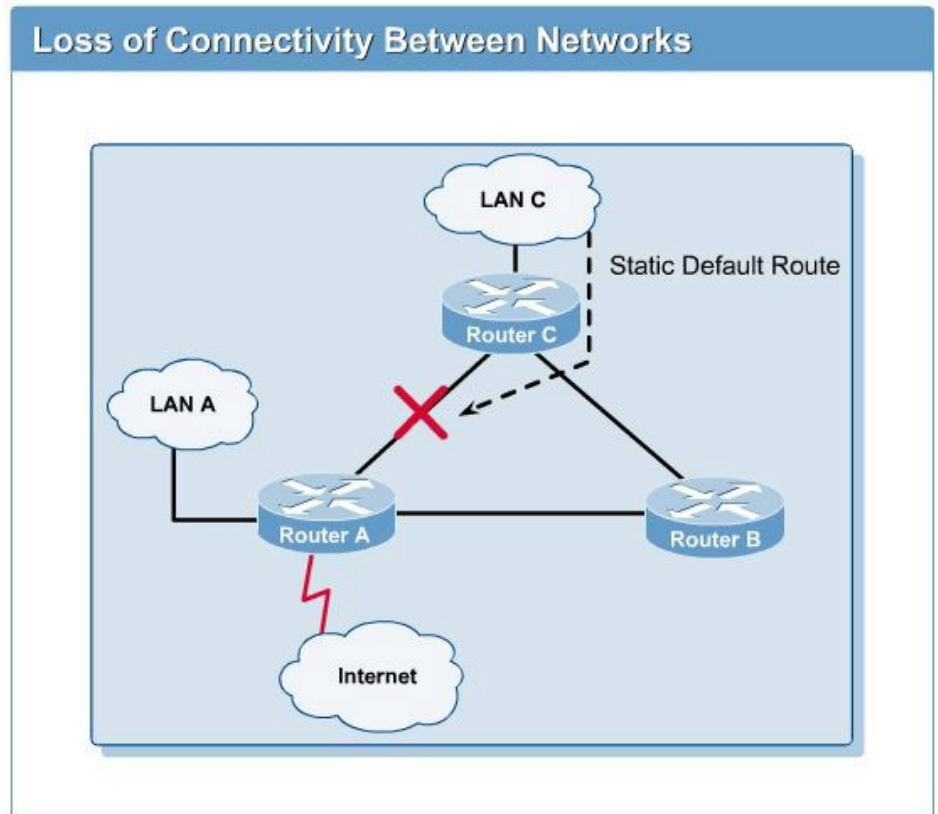
distance to target in hops

sending interface

(netstat -r)

Loss of Connectivity

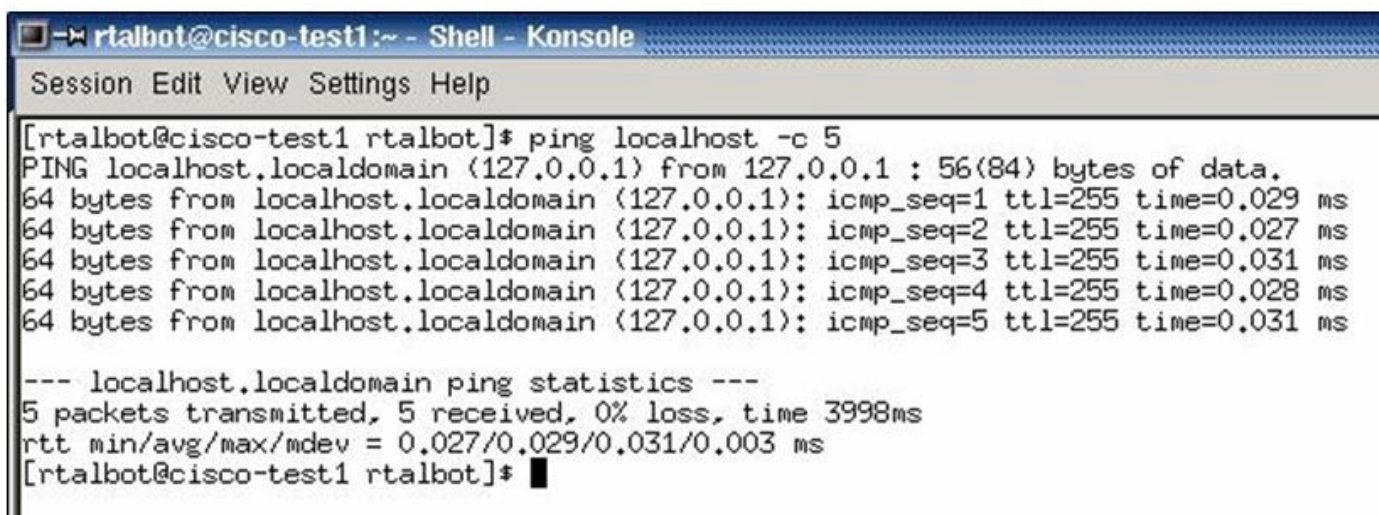
- La perdita di connessione può essere causata da hardware e / o software .
La prima regola di risoluzione dei problemi è quello di verificare la presenza di connettività fisica.
- Accertarsi che i cavi siano correttamente collegati sia a estremità, che l'adattatore di rete funzioni controllando la spia del collegamento sul NIC, che le luci dell'hub's status siano accese, e che i problemi di rete non sono semplicemente causati da un difetto di hardware



Using TCP/IP Utilities

- La prima operazione per controllare un problema di connettività sospetta è il ping dell'host (Packet internetworking Groper).
- Si invia un messaggio (Echo Request) a un host di destinazione usando ICMP (Internet Control Message Protocol). Il destinatario risponde con un ICMP Echo Reply.
- Se si riceve una risposta, la connessione fisica tra i due computer è integro e funzionante.
- La risposta di successo significa anche che il sistema di chiamata può raggiungere Internet.
- Il tempo di ping termine si riferisce alla quantità di tempo che intercorre tra l'invio della richiesta di echo request e ricevimento della Echo Reply.
- Un tempo di ping basso indica una connessione veloce.

Using TCP/IP Utilities



```
rtalbot@cisco-test1:~ - Shell - Konsole
Session Edit View Settings Help

[rtalbot@cisco-test1 rtalbot]$ ping localhost -c 5
PING localhost.localdomain (127.0.0.1) from 127.0.0.1 : 56(84) bytes of data.
64 bytes from localhost.localdomain (127.0.0.1): icmp_seq=1 ttl=255 time=0.029 ms
64 bytes from localhost.localdomain (127.0.0.1): icmp_seq=2 ttl=255 time=0.027 ms
64 bytes from localhost.localdomain (127.0.0.1): icmp_seq=3 ttl=255 time=0.031 ms
64 bytes from localhost.localdomain (127.0.0.1): icmp_seq=4 ttl=255 time=0.028 ms
64 bytes from localhost.localdomain (127.0.0.1): icmp_seq=5 ttl=255 time=0.031 ms

--- localhost.localdomain ping statistics ---
5 packets transmitted, 5 received, 0% loss, time 3998ms
rtt min/avg/max/mdev = 0.027/0.029/0.031/0.003 ms
[rtalbot@cisco-test1 rtalbot]$
```

- Pathping è un utility per Windows che combina le caratteristiche di ping con quelli di tracer, con informazioni aggiuntive.

C:\Documents and Settings\Sandro.AM-V1>pathping www.unive.it

Rilevazione route verso www.unive.it [157.138.7.88]

su un massimo di 30 punti di passaggio:

```
0  am-v1 [192.168.2.109]
1  192.168.2.1
2  homegate.homenet.telecomitalia.it [192.168.1.1]
3  192.168.100.1
4  host125-158-static.36-88-b.business.telecomitalia.it [88.36.158.125]
5  217.141.109.208
6  172.17.5.157
7  151.99.98.186
8  r-rm197-vl3.opb.interbusiness.it [151.99.29.151]
9  85.36.9.134
10 garr2-nap.namex.it [193.201.29.15]
11 rt1-bo1-rt-rm2.rm2.garr.net [193.206.141.5]
12 rt1-bo1-rt-pd1.pd1.garr.net [193.206.134.90]
13 rt-pd1-rc-ve-2.ve.garr.net [193.206.134.154]
14  *      *      *
```

Treviso

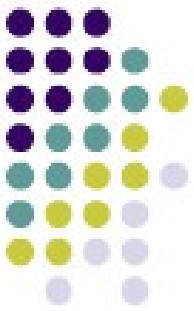
Roma

Padova
Venezia

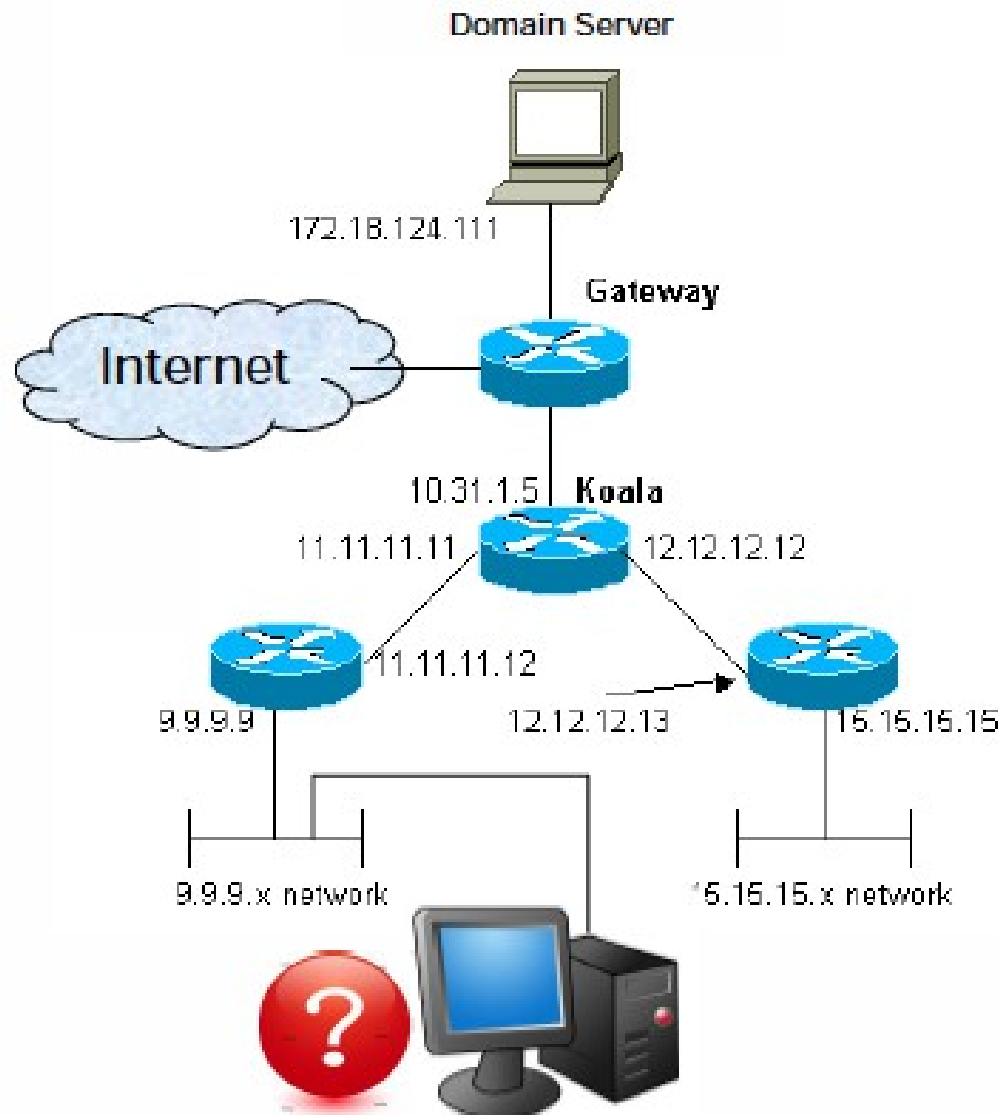
Statistiche di calcolo per 350 secondi...

Hop	RTT	Da orig. a qui Persi/Inv.= Pct	questo nodo/collegamento Persi/Inv.= Pct	Indir.	
0				am-v1 [192.168.2.109]	0/ 100 = 0%
1	0ms	0/ 100 = 0%	0/ 100 = 0%	192.168.2.1	0/ 100 = 0%
2	1ms	0/ 100 = 0%	0/ 100 = 0%	telecomitalia.it [192.168.1.1]	0/ 100 = 0%
3	199ms	0/ 100 = 0%	0/ 100 = 0%	192.168.100.1	0/ 100 = 0%
4	205ms	0/ 100 = 0%	0/ 100 = 0%	hos.business.it [88.36.158.125]	0/ 100 = 0%
5	205ms	0/ 100 = 0%	0/ 100 = 0%	217.141.109.208	0/ 100 = 0%
6	209ms	0/ 100 = 0%	0/ 100 = 0%	172.17.5.157	0/ 100 = 0%
7	215ms	0/ 100 = 0%	0/ 100 = 0%	151.99.98.186	0/ 100 = 0%
8	212ms	0/ 100 = 0%	0/ 100 = 0%	interbusiness.it [151.99.29.151]	0/ 100 = 0%
9	222ms	0/ 100 = 0%	0/ 100 = 0%	85.36.9.134	0/ 100 = 0%
10	---	100/ 100 =100%	100/ 100 =100%	garr2-nap.name.it [193.201.29.15]	0/ 100 = 0%
11	229ms	0/ 100 = 0%	0/ 100 = 0%	rt1-bo1.garr.net [193.206.141.5]	0/ 100 = 0%
12	225ms	0/ 100 = 0%	0/ 100 = 0%	pd1.garr.net [193.206.134.90]	0/ 100 = 0%
13	227ms	0/ 100 = 0%	0/ 100 = 0%	ve.garr.net [193.206.134.154]	100/ 100 =100%
14	---	100/ 100 =100%	0/ 100 = 0%	am-v1 [0.0.0.0]	

Rilevazione completata.



Using TCP/IP Utilities



1. hostname
2. ipconfig
3. ping 127.0.0.1
4. ping localhost
5. ping 9.9.9.1
6. ping 9.9.9.9
7. ping 11.11.11.12
8. ping 11.11.11.11
9. ping myName
10. ping remoteName

Using TCP/IP Utilities

- Il comando traceroute è usata per scoprire il percorso da un pacchetto d prova per raggiungere la sua destinazione (in Linux).
- Traceroute mostra tutti i router attraverso cui il pacchetto passa mentre viaggia attraverso la rete dall'invio del computer al computer di destinazione.
- Questo è utile per determinare a che punto è la connettività (persa o rallentata).

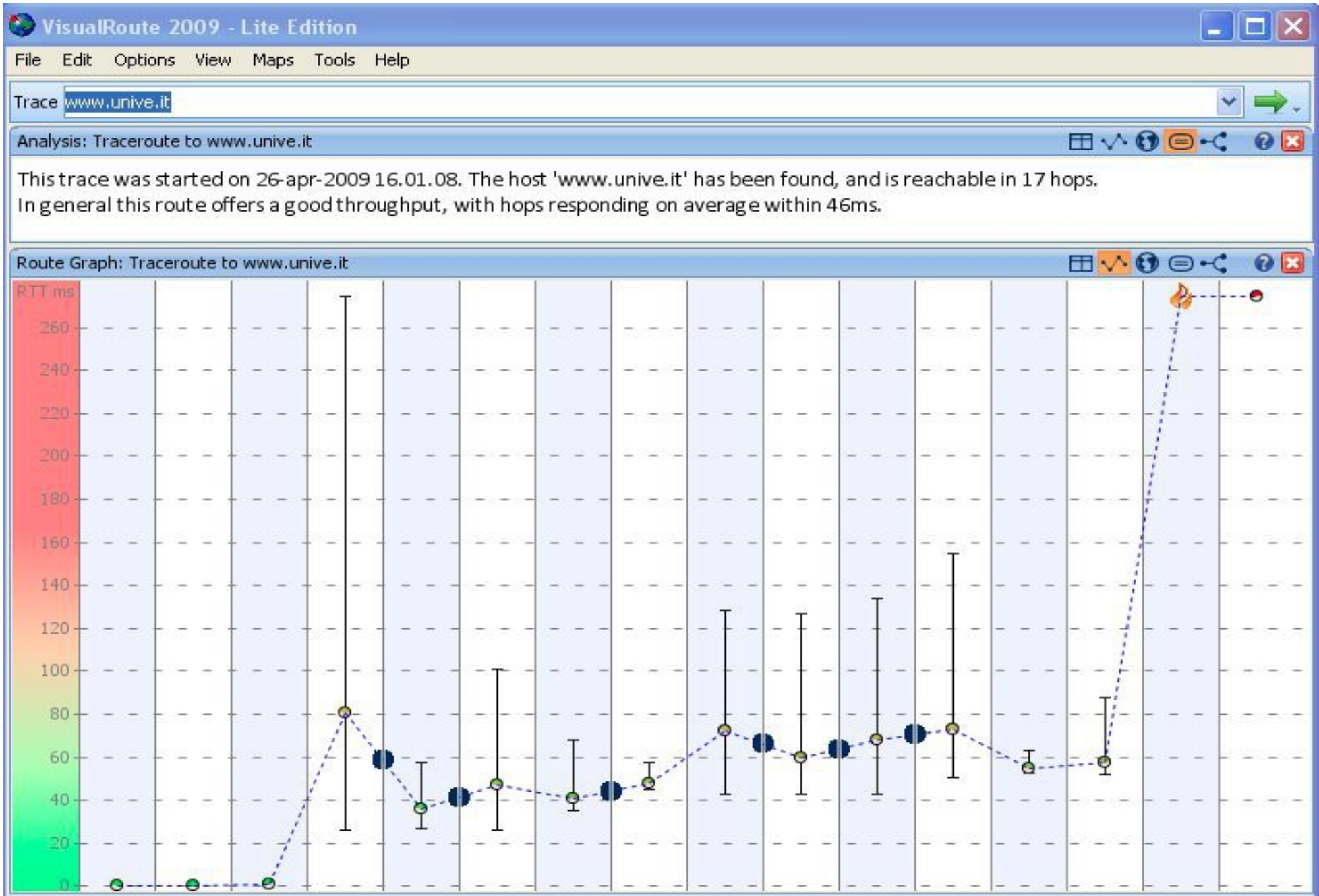
```
[rtalbot@cisco-test1 rtalbot]$ traceroute 168.2.221.165
traceroute to 168.2.221.165 (168.2.221.165), 30 hops max,
38 bytes packets
 1 phx2-00-gw1 (64.101.115.2)  0.509 mx  0.494 mx  0.470 ms
 2 phx2-wan-gw1-fe-0-0 (10.95.9.148)  1.046 mx  1.153 mx  1.318 ms
 3 rwcidc-wan-gw1-m5 (10.95.254.57) 34.755 ms 24.831 ms 25.669 ms
 4 rwcidc-rbb-gw2-fa-3-1 (10.92.253.22) 24.661 ms 22.265 ms 25.894 ms
 5 sjck-rbb-gw2 (171.69.7.221) 27.324 ms 27.659 ms 29.234 ms
 6 js-wall-2 (171.69.7.174) 25.096 ms 26.343 ms 26.182 ms
 7 sjck-dirty-gw1 (128.107.240.193) 26.326 ms 24.868 ms 27.253 ms
 8 * * *
```


Using TCP/IP Utilities

```
C:\Documents and Settings\Sandro.AM-V1>tracert www.unive.it
```

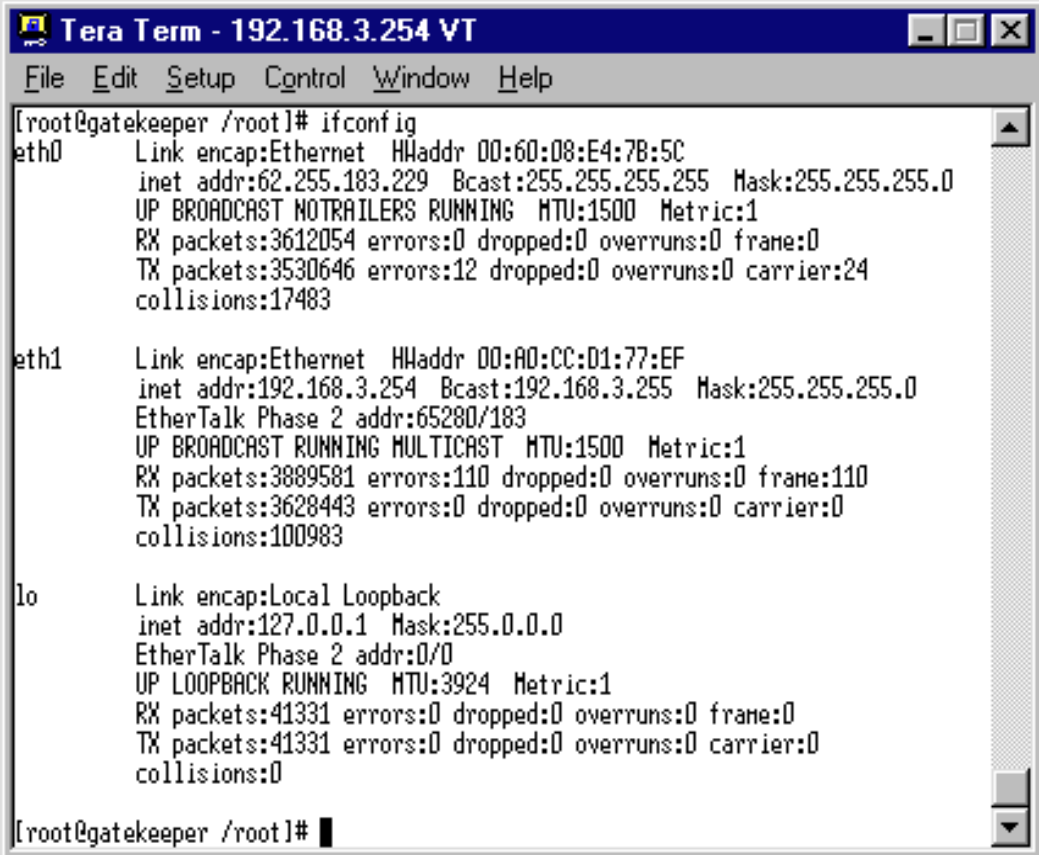
```
Rilevazione instradamento verso www.unive.it [157.138.7.88]  
su un massimo di 30 punti di passaggio:
```

1	<1 ms	<1 ms	<1 ms	192.168.2.1
2	1 ms	1 ms	1 ms	homegate.homenet.telecomitalia.it [192.168.1.1]
3	77 ms	100 ms	70 ms	192.168.100.1
4	36 ms	55 ms	102 ms	business.telecomitalia.it [88.36.158.125]
5	85 ms	58 ms	53 ms	217.141.109.208
6	105 ms	80 ms	76 ms	172.17.5.157
7	133 ms	101 ms	52 ms	151.99.98.186
8	103 ms	125 ms	145 ms	r-rm197-v13.opb.interbusiness.it [151.99.29.151]
9	67 ms	107 ms	109 ms	85.36.9.134
10	126 ms	117 ms	86 ms	garr2-nap.namex.it [193.201.29.15]
11	107 ms	108 ms	129 ms	rt1-bo1-rt-rm2.rm2.garr.net [193.206.141.5]
12	277 ms	265 ms	256 ms	rt1-bo1-rt-pd1.pd1.garr.net [193.206.134.90]
13	304 ms	211 ms	212 ms	rt-pd1-rc-ve-2.ve.garr.net [193.206.134.154]
14	*	*	*	Richiesta scaduta.



Using TCP/IP Utilities

- ifconfig (comando) permette la visualizzazione e cambiamento della configurazione di un interfaccia di rete associato con un dato dispositivo ethernet



```
Tera Term - 192.168.3.254 VT
File Edit Setup Control Window Help
[root@gatekeeper /root]# ifconfig
eth0      Link encap:Ethernet  HWaddr 00:60:08:E4:78:5C
          inet addr:62.255.183.229  Bcast:255.255.255.255  Mask:255.255.255.0
          UP BROADCAST NOTRAILERS RUNNING MTU:1500 Metric:1
          RX packets:3612054 errors:0 dropped:0 overruns:0 frame:0
          TX packets:3530646 errors:12 dropped:0 overruns:0 carrier:24
          collisions:17483
eth1      Link encap:Ethernet  HWaddr 00:AD:CC:01:77:EF
          inet addr:192.168.3.254  Bcast:192.168.3.255  Mask:255.255.255.0
          EtherTalk Phase 2 addr:65280/183
          UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
          RX packets:3889581 errors:110 dropped:0 overruns:0 frame:110
          TX packets:3628443 errors:0 dropped:0 overruns:0 carrier:0
          collisions:100983
lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          EtherTalk Phase 2 addr:0/0
          UP LOOPBACK RUNNING MTU:3924 Metric:1
          RX packets:41331 errors:0 dropped:0 overruns:0 frame:0
          TX packets:41331 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0
[root@gatekeeper /root]#
```

Using TCP/IP Utilities

- Per avere un elenco più sintetico:

```
$ ifconfig -s
```

- Per attivare/disattivare una interfaccia:

```
$ ifconfig eth0 up
```

```
$ ifconfig eth0 down
```

- Per assegnare un indirizzo IP / subnet mask:

```
$ ifconfig eth0 192.168.1.3 netmask 255.255.255.0
```

- Per vedere tutte le interfacce, anche quelle non attive:

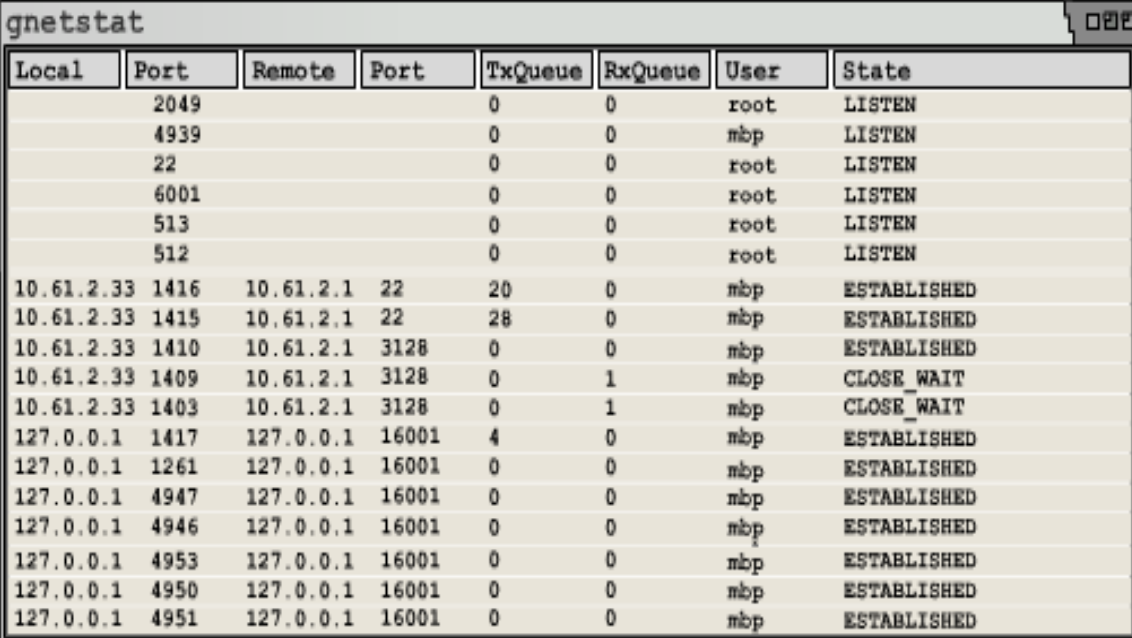
```
$ ifconfig -a
```

- Per attivare/disattivare la modalità promiscua (monitor):

```
$ ifconfig -promisc
```

Using TCP/IP Utilities

- L'utility netstat visualizza tutte le connessioni TCP attive, porte su cui il computer è in ascolto, Ethernet statistiche, la tabella di routing IP, le statistiche IPv4 (per l'IP, ICMP, TCP, e UDP), e le statistiche IPv6 (per i IPv6, ICMPv6, TCP su IPv6 e UDP su Ipv6 protocolli).



The screenshot shows a window titled "gnetstat" with a table of network connections. The table has eight columns: Local, Port, Remote, Port, TxQueue, RxQueue, User, and State. The data is as follows:

Local	Port	Remote	Port	TxQueue	RxQueue	User	State
	2049			0	0	root	LISTEN
	4939			0	0	nbp	LISTEN
	22			0	0	root	LISTEN
	6001			0	0	root	LISTEN
	513			0	0	root	LISTEN
	512			0	0	root	LISTEN
10.61.2.33	1416	10.61.2.1	22	20	0	nbp	ESTABLISHED
10.61.2.33	1415	10.61.2.1	22	28	0	nbp	ESTABLISHED
10.61.2.33	1410	10.61.2.1	3128	0	0	nbp	ESTABLISHED
10.61.2.33	1409	10.61.2.1	3128	0	1	nbp	CLOSE_WAIT
10.61.2.33	1403	10.61.2.1	3128	0	1	nbp	CLOSE_WAIT
127.0.0.1	1417	127.0.0.1	16001	4	0	nbp	ESTABLISHED
127.0.0.1	1261	127.0.0.1	16001	0	0	nbp	ESTABLISHED
127.0.0.1	4947	127.0.0.1	16001	0	0	nbp	ESTABLISHED
127.0.0.1	4946	127.0.0.1	16001	0	0	nbp	ESTABLISHED
127.0.0.1	4953	127.0.0.1	16001	0	0	nbp	ESTABLISHED
127.0.0.1	4950	127.0.0.1	16001	0	0	nbp	ESTABLISHED
127.0.0.1	4951	127.0.0.1	16001	0	0	nbp	ESTABLISHED



Il comando netstat

```
$ netstat -natup
```

- n mostra gli indirizzi IP e il numero della porta al posto dei relativi
- a mostra anche le porte in ascolto
- t mostra le porte che usano TCP
- u mostra le porte che usano UDP
- p mostra il PID e il nome del processo in ascolto.

```
alessandro@laptop:~$ netstat -natup
Active Internet Connections (servers and established)
Proto Recv-Q Send-Q Local Address Foreign Address State PID/Program name
tcp      0      0 127.0.0.1:631 0.0.0.0:* LISTEN -
tcp      0      0 192.168.2.2:80 0.0.0.0:* LISTEN 7658/apache2
udp      0      0 0.0.0.0:5353 0.0.0.0:* -
udp      0      0 0.0.0.0:68 0.0.0.0:* -
```

tipo di
protocollo

bytes non
ancora acquisiti

bytes non ancora
riscontrati

lato Local
del socket

lato Remote
del socket

proprietario
del socket

stato del socket
non presente per UDP e raw mode



Il comando netstat

Spiegazione riga per riga:

Proto	Recv-Q	Send-Q	Local Address	Foreign Address	State	PID/Program name
tcp	0	0	127.0.0.1:631	0.0.0.0:*	LISTEN	-

All'indirizzo locale di loopback 127.0.0.1 c'è un servizio in ascolto sulla porta 631 (corrispondente a IPP, Internet Printing Protocol) . Questo servizio è dichiarato pronto a ricevere connessioni provenienti da qualsiasi indirizzo e da qualsiasi porta, ma in realtà risponde solo a richieste della macchina locale.

Proto	Recv-Q	Send-Q	Local Address	Foreign Address	State	PID/Program name
tcp	0	0	192.168.2.2:80	0.0.0.0:*	LISTEN	7658/apache2 -

Sull'indirizzo 192.168.2.2 c'è un servizio in ascolto sulla porta 80 (corrispondente a HTTP) . Questo servizio (server web) è pronto a ricevere connessioni provenienti da qualsiasi indirizzo e da qualsiasi porta.



Il comando netstat

Proto	Recv-Q	Send-Q	Local Address	Foreign Address	State	PID/Program name
udp	0	0	0.0.0.0:5353	0.0.0.0:*	-	

Al generico indirizzo locale (simile a 127.0.0.1) è stata aperta una porta verso un indirizzo non ancora noto (corrispondente a MDNS, Multicast DNS) . Questo servizio è frutto di una richiesta broadcast della macchina locale.

Proto	Recv-Q	Send-Q	Local Address	Foreign Address	State	PID/Program name
udp	0	0	0.0.0.0:68	0.0.0.0:*	-	

Al generico indirizzo locale (simile a 127.0.0.1) è stata aperta una porta verso un indirizzo non ancora noto (corrispondente a BOOTP Client, Bootstrap Protocol Client). Questo servizio è frutto di una richiesta broadcast della macchina locale di ricevere una configurazione IP iniziale.



Il comando netstat

```
C:\> netstat -n -a -p TCP -p UDP -o
```

```
C:\Documents and Settings\Sandro.AM-VI>netstat -n -a -p TCP -p UDP -o
```

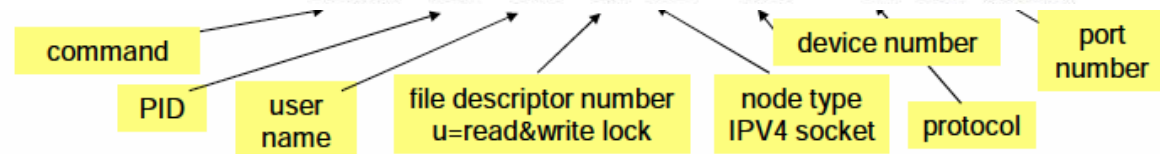
Connessioni attive

Proto	Indirizzo locale	Indirizzo esterno	PID	
UDP	0.0.0.0:445	*:*	4	microsoft-DS
UDP	0.0.0.0:500	*:*	936	isakmp UDP
UDP	0.0.0.0:1035	*:*	1420	MX-XR RPC
UDP	0.0.0.0:1072	*:*	1420	CARDAX
UDP	0.0.0.0:1073	*:*	1420	Bridge Control
UDP	0.0.0.0:1074	*:*	1420	Warmspot Management Protocol
UDP	0.0.0.0:1075	*:*	1420	RDRMSHC
UDP	0.0.0.0:1076	*:*	1420	DAB STI-C
UDP	0.0.0.0:1077	*:*	1420	IMGames
UDP	0.0.0.0:1078	*:*	1420	Avocent Proxy Protocol
UDP	0.0.0.0:1079	*:*	1420	ASPROVATalk
UDP	0.0.0.0:1080	*:*	1420	Socks
UDP	0.0.0.0:4500	*:*	936	IPsec NAT-Traversal
UDP	127.0.0.1:123	*:*	1304	Network Time Protocol
UDP	127.0.0.1:1033	*:*	472	local netinfo port
UDP	127.0.0.1:1900	*:*	1592	SSDP
UDP	192.168.2.109:123	*:*	1304	Network Time Protocol
UDP	192.168.2.109:137	*:*	4	NETBIOS Name Service
UDP	192.168.2.109:138	*:*	4	NETBIOS Datagram Service
UDP	192.168.2.109:1900	*:*	1592	SSDP

Using TCP/IP Utilities

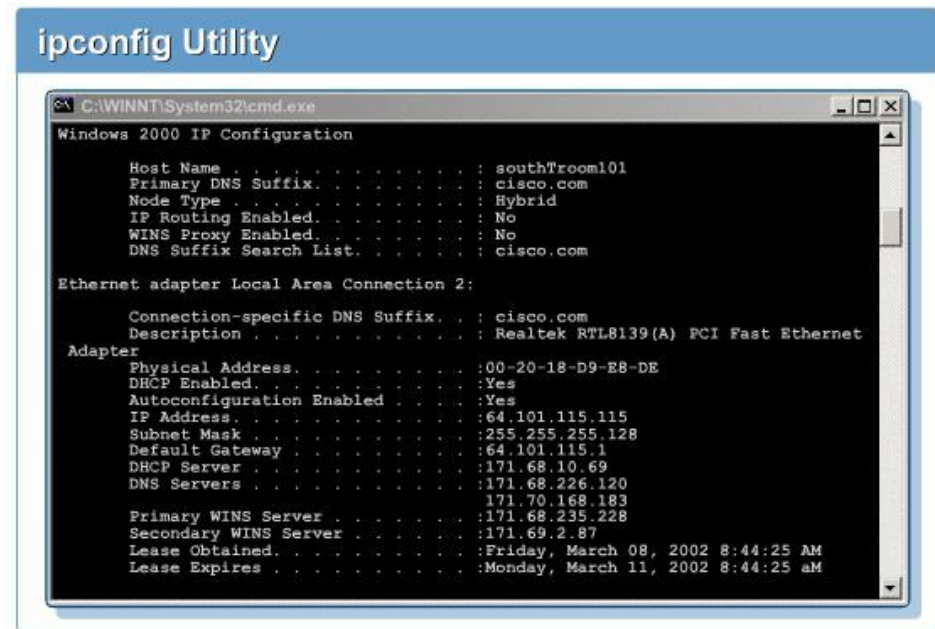
- Isof è in grado di identificare le risorse connesse in rete e quali processi possono essere loro bloccarsi.
- il Isof (Lista aperta Files) liste informazioni su file (!), Che sono aperto da l'esecuzione processi.

```
root@:~# lsof -i
COMMAND      PID    USER   FD   TYPE    DEVICE  SIZE  NODE  NAME
httpd        2530  nobody  3u    IPv4    4117          TCP *:http (LISTEN)
inetd        6344   root    4u    IPv4    4013          TCP *:time (LISTEN)
inetd        6344   root    5u    IPv4    4014          UDP *:time
inetd        6344   root    6u    IPv4    4015          UDP *:biff
inetd        6344   root    7u    IPv4    4016          TCP *:auth (LISTEN)
sshd         6348   root    3u    IPv4    4022          TCP *:ssh (LISTEN)
sendmail     6365   root    4u    IPv4    36184701      TCP *:smtp (LISTEN)
sendmail     6365   root    5u    IPv4    36184702      TCP *:submission (LISTEN)
ntpd         6380   root    16u   IPv4    4073          UDP *:ntp
ntpd         6380   root    17u   IPv4    4074          UDP localhost:ntp
mysqld       6415   mysql   3u    IPv4    4109          TCP *:3306 (LISTEN)
mysqld       6417   mysql   3u    IPv4    4109          TCP *:3306 (LISTEN)
mysqld       6418   mysql   3u    IPv4    4109          TCP *:3306 (LISTEN)
httpd        6419   root    3u    IPv4    4117          TCP *:http (LISTEN)
mysqld       6421   mysql   3u    IPv4    4109          TCP *:3306 (LISTEN)
mysqld       6422   mysql   3u    IPv4    4109          TCP *:3306 (LISTEN)
mysqld       6423   mysql   3u    IPv4    4109          TCP *:3306 (LISTEN)
mysqld       6433   mysql   3u    IPv4    4109          TCP *:3306 (LISTEN)
mysqld       6435   mysql   3u    IPv4    4109          TCP *:3306 (LISTEN)
mysqld       6437   mysql   3u    IPv4    4109          TCP *:3306 (LISTEN)
mysqld       6439   mysql   3u    IPv4    4109          TCP *:3306 (LISTEN)
asterisk     6451   root    9u    IPv4    4196          TCP *:5038 (LISTEN)
```



Using TCP/IP Utilities

- Il comando ipconfig viene utilizzato in Windows NT e Windows 2000 per visualizzare l'indirizzo IP, la subnet mask, e il gateway predefinito per i quali una scheda di rete è configurata.
- per ulteriori dettagliate informazioni, è utilizzato
- /all



The screenshot shows the 'ipconfig Utility' window, which is a command prompt window titled 'C:\WINNT\System32\cmd.exe'. The output of the 'ipconfig' command is displayed, showing the configuration for 'Ethernet adapter Local Area Connection 2:'. The configuration includes the host name 'southTrooml01', primary DNS suffix 'cisco.com', node type 'Hybrid', IP routing enabled, WINS proxy enabled, and DNS suffix search list 'cisco.com'. The adapter's physical address is '00-20-18-D9-E8-DE', and it is a 'Realtek RTL8139(A) PCI Fast Ethernet' adapter. The IP address is '64.101.115.115', the subnet mask is '255.255.255.128', and the default gateway is '64.101.115.1'. The DHCP server is '171.68.10.69', and the DNS servers are '171.68.226.120' and '171.70.158.183'. The primary WINS server is '171.68.235.228', and the secondary WINS server is '171.69.2.87'. The lease was obtained on 'Friday, March 08, 2002 8:44:25 AM' and expires on 'Monday, March 11, 2002 8:44:25 AM'.

```
ipconfig Utility

C:\WINNT\System32\cmd.exe
Windows 2000 IP Configuration

Host Name . . . . . : southTrooml01
Primary DNS Suffix . . . . . : cisco.com
Node Type . . . . . : Hybrid
IP Routing Enabled. . . . . : No
WINS Proxy Enabled. . . . . : No
DNS Suffix Search List. . . . . : cisco.com

Ethernet adapter Local Area Connection 2:

Connection-specific DNS Suffix. . . : cisco.com
Description . . . . . : Realtek RTL8139(A) PCI Fast Ethernet
Adapter
Physical Address. . . . . : 00-20-18-D9-E8-DE
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . . : Yes
IP Address. . . . . : 64.101.115.115
Subnet Mask . . . . . : 255.255.255.128
Default Gateway . . . . . : 64.101.115.1
DHCP Server . . . . . : 171.68.10.69
DNS Servers . . . . . : 171.68.226.120
                          171.70.158.183
Primary WINS Server . . . . . : 171.68.235.228
Secondary WINS Server . . . . . : 171.69.2.87
Lease Obtained. . . . . : Friday, March 08, 2002 8:44:25 AM
Lease Expires . . . . . : Monday, March 11, 2002 8:44:25 AM
```

Problem-Solving Guidelines

- Risoluzione dei problemi di una rete necessita di competenze problem-solving .
- L'utilizzo di un metodo strutturato per rilevare, analizzare, e affrontare ogni problema , aumenta la probabilità di successo e risoluzione dei problemi.
- Questi passaggi devono essere seguiti:
 - Raccogliere informazioni
 - Analizzare le informazioni
 - Formulare e attuare un piano di "trattamento"
 - Test per verificare i risultati del trattamento
 - Documentare tutto

Windows 2000 Diagnostic Tools

- Gli strumenti di diagnostica di rete per Microsoft Windows 2000 Server includono ipconfig, nbtstat, netstat, nslookup, ping e tracer.
- nbtstat.exe E' UN STRUMENTO Utile per risolvere i PROBLEMI relativi alla risoluzione di nomi NetBIOS su TCP / IP.

```
C:\Documents and Settings\Sandro.AM-V1>nbtstat -n

Connessione alla rete locale (LAN):
Indirizzo IP nodo: [192.168.2.109] ID ambito: []

          Tabella nomi locali NetBIOS

      Nome                Tipo                Stato
-----
AM-V1          <00> UNICO          Registrato
WORKGROUP      <00> GRUPPO        Registrato
AM-V1          <20> UNICO          Registrato
WORKGROUP      <1E> GRUPPO        Registrato
```

Windows 2000 Diagnostic Tools

- Nslookup.exe è uno strumento di amministrazione da riga di comando per test e la risoluzione dei problemi dei server DNS.
- Nslookup.exe può essere eseguito in due modalità: interattiva e non interattiva. Modalità non interattiva è utile quando solo un singolo pezzo di dati deve essere restituito:

`nslookup [-option] [hostname] [server]`

- Per iniziare Nslookup.exe in modalità interattiva, digitare semplicemente "nslookup"

```
C:\> nslookup
Default Server: nameserver1.domain.com
Address: 10.0.0.1
>
```

Windows 2000 Diagnostic Tools

```
C:\nslookup www.google.it
```

```
Default Server: ns1.domain.com
```

```
Address: 10.0.0.1
```

```
Risposta da un server non di fiducia:
```

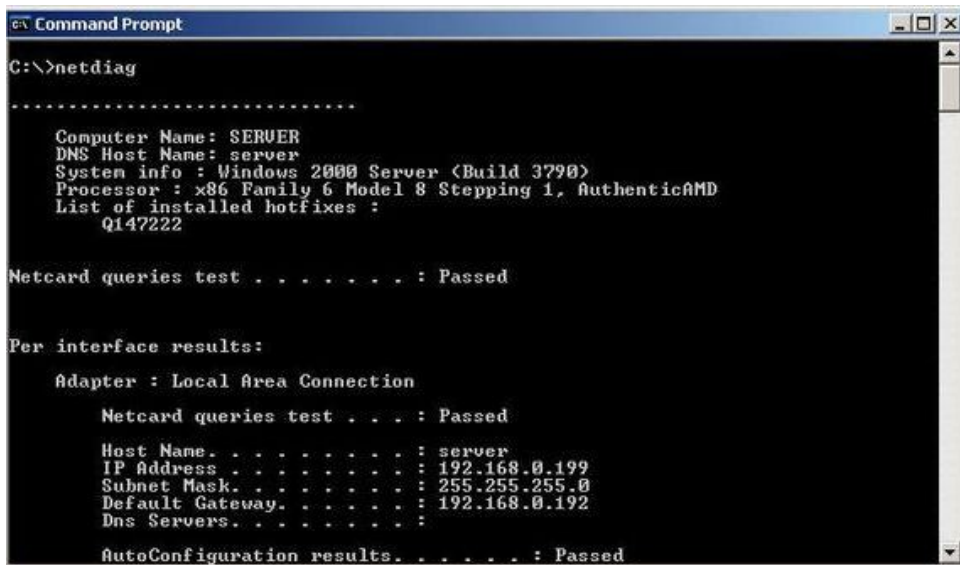
```
Nome:      www.l.google.com
```

```
Addresses: 74.125.43.104, 74.125.43.99, 74.125.43.103, 74.125.43.147
```

```
Aliases:   www.google.it, www.google.com
```

Windows 2000 Diagnostic

- Il comando Netdiag esegue un serie standard di test di rete e genera un report dei risultati.



```
C:\>netdiag

.....

Computer Name: SERVER
DNS Host Name: server
System info : Windows 2000 Server (Build 3790)
Processor : x86 Family 6 Model 8 Stepping 1, AuthenticAMD
List of installed hotfixes :
    Q147222

Netcard queries test . . . . . : Passed

Per interface results:

  Adapter : Local Area Connection

    Netcard queries test . . . : Passed

    Host Name . . . . . : server
    IP Address . . . . . : 192.168.0.199
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . : 192.168.0.192
    Dns Servers . . . . . :

  AutoConfiguration results . . . . . : Passed
```

Command Flag	What It Means
/q	Quiet output (errors only)
/v	Provides verbose output. More detailed information is provided.
/l	Logs output to Netdiag.log
/debug	Provides even more verbose output.
/d:<DomainName>	Finds a DC in the specified domain.
/fix	Fixes trivial problems.
/DcAccountEnum	Enumerates DC machine accounts.
/test:<test name>	Tests only this test. Non -skippable tests will still be run

Windows 2000 Diagnostic Tools

- Il comando è un pathping combinazione del comando ping e il comando tracert.

```
C:\>pathping www.infomedia.it

Rilevazione route verso danteweb.infomedia.it [194.243.78.46]
su un massimo di 30 punti di passaggio:
 0  geonbook [138.70.192.180]
 1  138.70.20.220
 2  138.70.250.53
 3  * *
Statistiche di calcolo per 75 secondi...
Da orig. a qui questo nodo/collegamento
Hop RTT  Persi/Inv.= Pct  Persi/Inv.= Pct  Indir.
 0      0/ 100 = 0%    0/ 100 = 0%    geonbook [138.70.192.180]
 1    1ms    0/ 100 = 0%    0/ 100 = 0%    138.70.20.220
 2   32ms    0/ 100 = 0%    0/ 100 = 0%    138.70.250.53
 3    ---  100/ 100 =100%   0/ 100 = 0%    geonbook [0.0.0.0]

Rilevazione completata.
```

Command Flag	What It Means
-n	Specifies to not resolve addresses to host names.
-h <i>maximum-hops</i>	Specifies the maximum number of hops to search for target.
-g <i>host-list</i>	Specifies the loose source route along host-list.
-p <i>period</i>	Specifies the wait period in milliseconds between pings.
-q <i>num-queries</i>	Specifies the number of queries per hop.
-w <i>timeout</i>	Specifies the wait timeout milliseconds for each reply.
-T	Tests connectivity to each hop with Layer 2 priority tags.
-R	Tests whether each hop is RSVP aware.