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

Hardware Problems

Although a few problems are due to a combination of factors, most can be isolated in origin to one of these:

- **Hardware** – A component of system hardware has malfunctioned, or is expected but not present.
- **Kernel** – A bug or lack of functionality in the system kernel sometimes causes problems of ambiguous origin.
- **Application software** – User level application software or command utilities may behave strangely, or simply collapse.
- **Configuration** – System services or application software may be misconfigured.
- **User error** – One of the most frequent sources of error conditions is caused by computer users attempting to do something the wrong way.

Hardware Problems

- Every sort of error condition may be categorized one of two ways, either **consistent** or **inconsistent**.
- Some hardware errors will be obvious. Other leaves traces that the kernel detects and records.
- Assuming an error is such that it does not crash the system, evidence might be left in the log file **/var/log/messages**, with the message prefixed by the word ***oops***.

```
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  rtalbot(uid=500)
```

Using System Utilities and System Status Tools

- Linux operating systems provide various system utilities and system status tools:
  - setserial
  - lpq
  - ifconfig
  - route
- The following utilities will return information about how the system or a file “should” be configured.

Using System Utilities and System Status Tools

- The **setserial** utility provides information and set options for the serial ports on the system.
- Typically the serial ports are **/dev/ttyS0** e /dev/ttyS1
- To obtain detailed information of a particular serial port:

#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

- The **lpq** command helps resolve printing problems.
- The command will display all the jobs that are waiting to be printed.
- If the print job that was submitted disappears from the queue then there is something wrong with the print queue

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

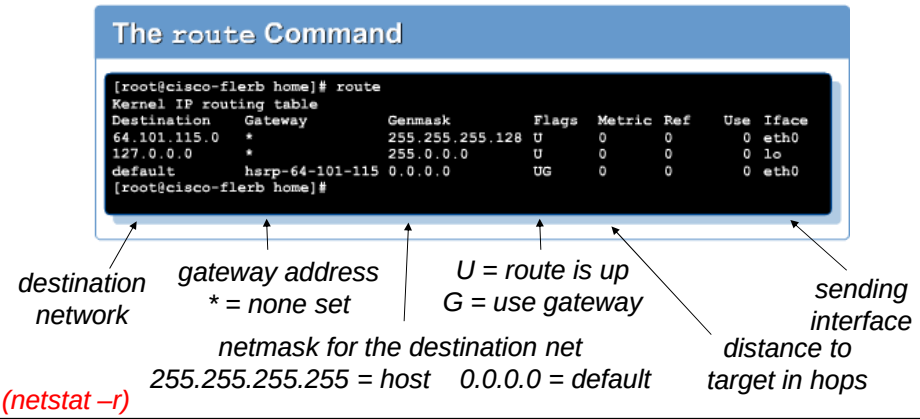
- The **ifconfig** command can be entered at the shell to return the current network interface configuration of the system.

The `ifconfig` Command

```
[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]#
```

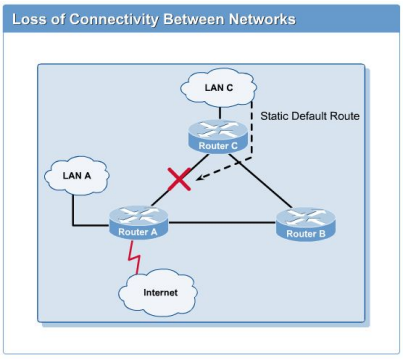
Using System Utilities and System Status Tools

- The **route** command displays or sets the information on the system's routing, which it uses to send information to particular IP addresses.



Loss of Connectivity

- Loss of connectivity can be hardware and/or software related. The first rule of troubleshooting is to check for physical connectivity.
- Ensure that the cables are properly plugged in at both ends, that the network adapter is functioning by checking the link light on the NIC, that the hub's status lights are on, and that the communication problem is not a simple hardware malfunction.



Using TCP/IP Utilities

- The first step in checking for a suspected connectivity problem is to **ping** (*Packet INternetworking Groper*) the host.
- It sends a message (*Echo Request*) to a destination host using ICMP (*Internet Control Message Protocol*). The destination responds with an ICMP Echo Reply.
- If a reply is received, the physical connection between the two computers is intact and working.
- The successful reply also signifies that the calling system can reach the Internet.
- The term *ping time* refers to the amount of time that elapses between the sending of the Echo Request and receipt of the Echo Reply.
- A low ping time indicates a fast connection.

Using TCP/IP Utilities

Ping Request and Response

rtalbot@cisco-test1:~ - Shell - Konsole

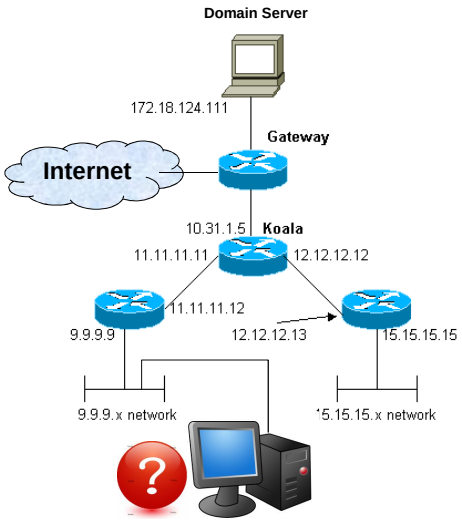
Session Edit View Settings Help

```
[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** is a Windows utility that combines the features of **ping** with those of **tracert**, with additional information.

```
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                                                    Treviso
  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                                                   Roma
  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]                   Padova
 13  rt-pd1-rc-ve-2.ve.garr.net [193.206.134.154]                   Venezia
 14     *        *        *
Statistiche di calcolo per 350 secondi...
            Da orig. a qui   questo nodo/collegamento
Hop  RTT    Persi/Inv.= Pct  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

- The **traceroute** command is used to discover the route taken by a packet to reach its destination (in Linux).
- **Traceroute** shows all the routers through which the packet passes as it travels through the network from sending computer to destination computer.
- This is useful for determining at what point connectivity is lost or slowed.

```
[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-vl3.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

- The **ifconfig** command allows viewing and changing the configuration of a network interface associated with a given ethernet device

```
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:E4:7B: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:A0:CC:D1:77: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:

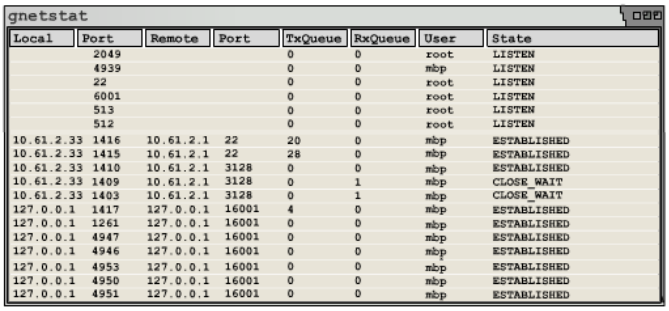
```
$ ifconfig -a
```

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

```
$ ifconfig -promisc
```

Using TCP/IP Utilities

- The **netstat** utility displays all active TCP connections, ports on which the computer is listening, Ethernet statistics, the IP routing table, IPv4 statistics (for the IP, ICMP, TCP, and UDP protocols), and IPv6 statistics (for the IPv6, ICMPv6, TCP over IPv6, and UDP over IPv6 protocols).

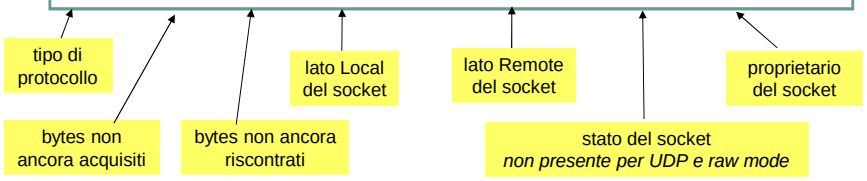


Il comando netstat

`$ 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:*              -
```



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-V1>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

- **lsof** is able to identify networking related resources and what processes may be locking them up.
- The lsof (LiSt Open Files) lists information about files (!!!) that are opened by the running processes.

```
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)
```

command

PID

user name

file descriptor number u=read&write lock

node type IPV4 socket

device number

protocol

port number

Using TCP/IP Utilities

- The **ipconfig** command is used in Windows NT and Windows 2000 to display the IP address, subnet mask, and default gateway for which a network adapter is configured.
- For more detailed information, the **/all** switch is used.

ipconfig Utility

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

        Host Name . . . . . . . . . . . . : southTroom101
        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
                                           171.70.168.183
        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

- Troubleshooting a network requires problem-solving skills.
- The use of a structured method to detect, analyze, and address each problem as it is encountered increases the likelihood of successful troubleshooting.
- These steps should be followed:
  - Gather information
  - Analyze the information
  - Formulate and implement a "treatment" plan
  - Test to verify the results of the treatment
  - Document everything

Windows 2000 Diagnostic Tools

- The network diagnostic tools for Microsoft Windows 2000 Server include **ipconfig**, **nbtstat**, **netstat**, **nslookup**, **ping**, and **tracert.**
- **nbtstat.exe** è un utile strumento 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** is a command-line administrative tool for testing and troubleshooting DNS servers.
- nslookup.exe can be run in two modes: interactive and noninteractive. **Noninteractive** mode is useful when only a single piece of data needs to be returned:

  nslookup [-option] [hostname] [server]

- To start nslookup.exe in **interactive** mode, simply type "nslookup“

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

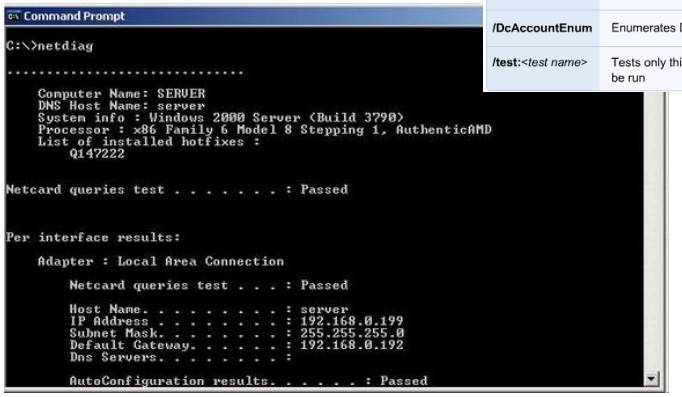
Windows 2000 Diagnostic Tools

```
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 Diagn

- The **Netdiag** command runs a standard set of network tests and generates a report of the results.

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

- The **pathping** command is a combination of the *ping* command and the *tracert* command.

Command Flag	What It Means
-n	Specifies to not resolve addresses to host names.
-h *maximum-hops*	Specifies the maximum number of hops to search for target.
-g *host-list*	Specifies the loose source route along host-list.
-p *period*	Specifies the wait period in milliseconds between pings.
-q *num-queries*	Specifies the number of queries per hop.
-w *timeout*	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.