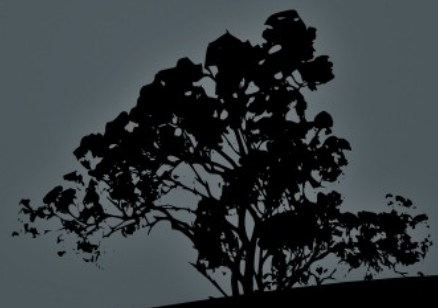
LPIC-1 102-400 – Lesson 16

109.3 Basic network troubleshooting

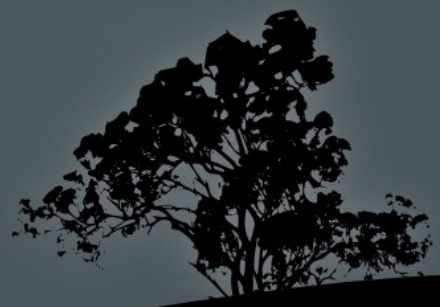
Problems with DHCP

- If a computer refuses to get an IP address from DHCP, or gets a 169.254.0.0/16 address this could mean that there is not working DHCP on the network
  - Try to manually set an available IP address from your network and give the correct netmask and gateway (**ip addr**/**ifconfig**)
  - Then try to communicate with another host in the same network (**ping**) like the default gateway



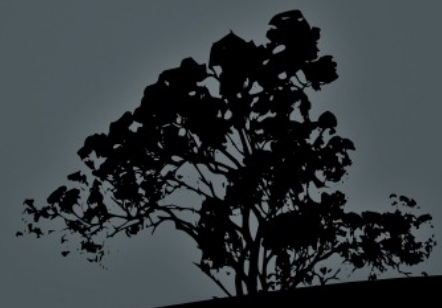
IP Address Conflict

- IP address conflict happens when we use the same IP in two or more nodes. This is one of the hardest problems to detect. When 2 or more nodes have the same IP address you will observe interruptions in their operation
  - Use **ping** from another computer and see if you get a reply. If you disconnect **(ifdown**) the suspect computer and you still get replies, this means that the IP address is in use somewhere else
  - Try to assign an available IP address from the correct network (**ip addr**/**ifconfig**) using the correct netmask and gateway, and try to re-enable the interface (**ifup**)



IP from another subnet

- Sometimes we may be confused and set an IP address that it is apparently from our own network but it is, in fact, on another network. For example 192.168.10.250 does not belong to 192.168.10.0/25
  - Try to calculate the boundaries of your network. The **ipcalc** command can be a valuable tool in such cases
  - Then try to set an IP address from your network and using the correct mask
  - Finally use **ping** to get an answer from other nodes in your network



Unreachable remote networks

- If you can communicate with nodes inside your own subnet but you cannot communicate with other subnets, this is a typical problem,related to the default gateway
  - The problem could be a gateway which is offline. Try to get an answer from it with **ping**
  - The wrong gateway may have been specified. Try to set the correct one with **ip ro add default via** after consulting your network administrator

Wrong hostname

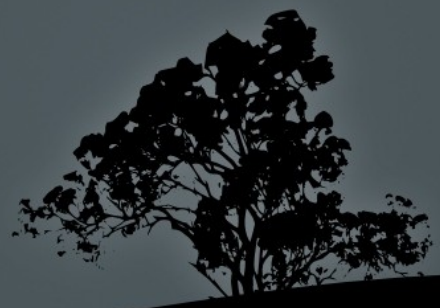
- Some network can pick up the hostname from the computer and set it up in their DNS. In such scenarios, if you have the wrong hostname, the other computers will not be able to connect to you using that hostname
  - Correct your hostname with the command **hostname**
  - Try to **ping** it from another node in the network
  - If it works make the hostname persistent by adding it in **/etc/hostname**

Problems with DNS

- If a system fails to resolve named to IP addresses, the reason can be the lost communication with the DNS server. If we can talk to an IP address but not the hostname this is a typical DNS problem
  - Try to ping the IP address of the host and then the hostname (**ping**)
  - If the IP address responds but not the hostname, check the communication with the DNS server with **ping** or try to send a DNS query to it with **host**, **dig** or **nslookup**. If that fails try sending a DNS query to a public DNS server such us 8.8.8.8 (Google DNS)

Check communication with remote networks

- If we fail to communicate with a remote node or network we should try to find the intermediate device that causes this problem.
  - The **ping** command can verify the problem but it does not help us find where exactly is the problem
  - To troubleshoot the problem we have to use **traceroute** or a similar command like **tracepath** or **mtr**



The `netstat` command

- The **netstat** is a utility for displaying active connections, active ports, the routing table and detailed statistics about network usage

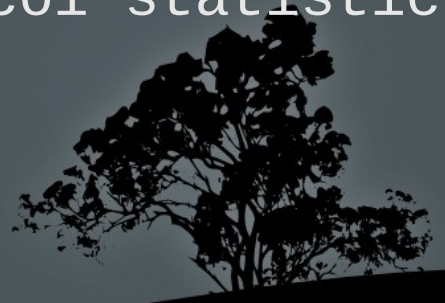
Options:

- `-i # interfaces list with statistics`
- `-s # detailed per protocol statistics`
- `-a # show all listening ports and active connections`
- `-l # show listening ports`
- `-p # show the process behind each connection or listening port`
- `-r # show routing table`
- `-n # numeric results. It does not resolve hostnames which means faster results`
- `-t # show TCP connections`
- `-u # show UDP communication`
- `-c # repeatedly show results every second`

NOTE: *in modern systems* ***netstat*** *is being phased out by the* ***ss*** *utility*

The `netstat` command

- # **netstat** # show all sockets, TCP, UDP and unix
- # **netstat -tuc** # continues update of TCP and UDP traffic
- # **netstat -tun** # numeric display of TCP and UDP traffic
- # **netstat -an** # show connections and ports in numeric form
- # **netstat -lnptu** # show listening TCP and UDP ports, in numeric form, along with programs that occupy these ports
- # **netstat -r** # show routing table
- # **netstat -i** # show interface and statistics
- # **netstat -s** # detailed, per protocol statistics



The `netstat` command

- **# netstat -tu** # show TCP and UDP connections

```
Proto Recv-Q Send-Q Local Address           Foreign Address         State
...
tcp        0      1 pcname.local:54992  iad04s01-in-f120.1e:www FIN_WAIT1
tcp        0      0 pcname.local:53464  ip-208-109-125-16:imap2 ESTABLISHED
tcp        0      0 pcname.local:59736  malena:imap2            ESTABLISHED
udp        0      0 localhost:46107         localhost:46107         ESTABLISHED
```

- **# netstat -tun** # show TCP and UDP connections in numeric form

```
Proto Recv-Q Send-Q Local Address           Foreign Address         State
...
tcp        0      0 192.168.2.11:54992      72.14.204.120:80        TIME_WAIT
tcp        0      0 192.168.2.11:53464      208.109.125.161:143     ESTABLISHED
tcp        0      0 192.168.2.11:59736      69.64.38.128:143        ESTABLISHED
udp        0      0 127.0.0.1:46107         127.0.0.1:46107         ESTABLISHED
```

The `netstat` command

- # **netstat -lnptu** # show listening TCP and UDP ports with applications

```
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/
   Program name
...
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN      977/
   sshd
tcp        0      0 127.0.0.1:631           0.0.0.0:*               LISTEN
   1782/cupsd
tcp        0      0 127.0.0.1:5432          0.0.0.0:*               LISTEN
   1535/postgres
tcp        0      0 127.0.0.1:3306          0.0.0.0:*               LISTEN
   1503/mysqld
tcp6       0      0 :::80                   :::*                    LISTEN
   2024/apache2
...
udp        0      0 0.0.0.0:68              0.0.0.0:*
   8054/dhclient
udp        0      0 0.0.0.0:123             0.0.0.0:*
   8178/ntpd
udp        0      0 0.0.0.0:137             0.0.0.0:*
   2231/nmbd
udp        0      0 192.168.2.11:138        0.0.0.0:*
   2231/nmbd
udp6       0      0 :::123                  :::*
   8178/ntpd
...
```

License