Intro to Networking Tools

References

https://www.tecmint.com/linux-network-configuration-and-troubleshooting-commands/
https://www.tecmint.com/8-linux-nslookup-commands-to-troubleshoot-dns-domain-name-server/

https://www.javatpoint.com/linux-nslookup

https://itsfoss.com/basic-linux-networking-commands/

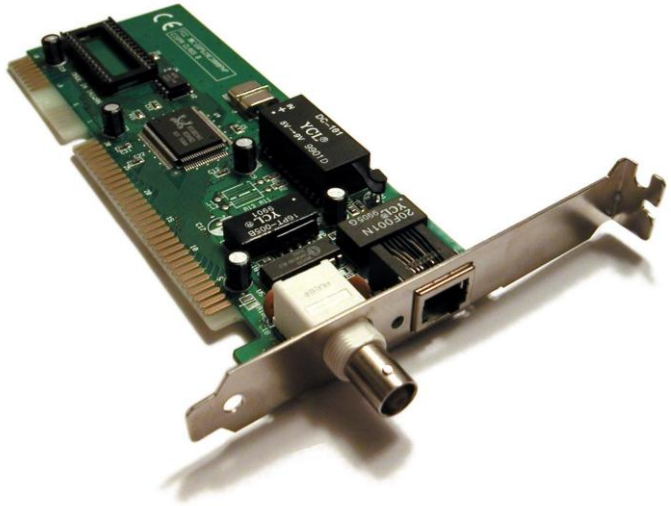
- ifconfig
  - **interface configurator (ifconfig)** is use to initialize an interface, assign IP Address to interface and enable or disable interface on demand.

```
# ifconfig

eth0      Link encap:Ethernet  HWaddr 00:0C:29:28:FD:4C
          inet addr:192.168.50.2  Bcast:192.168.50.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fe28:fd4c/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:6093 errors:0 dropped:0 overruns:0 frame:0
          TX packets:4824 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:6125302 (5.8 MiB)  TX bytes:536966 (524.3 KiB)
          Interrupt:18 Base address:0x2000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:8 errors:0 dropped:0 overruns:0 frame:0
```

- **Network Interface:**
- software interface to networking hardware.
- A network interface will usually have some form of network address (IP and MAC address, for instance)



- Enable / Disable Interface:

Enable eth0

```
# ifup eth0
```

Disable eth0

```
# ifdown eth0
```

- **eth0**, **lo** and **wlan0** are the names of the active network interfaces on the system.
- Additional Ethernet interfaces would be named **eth1**, **eth2**, etc.
- **lo** is the loopback interface. This is a special network interface that the system uses to communicate with itself.
- **wlan0** is the name of the first wireless network interface on the system. Additional wireless interfaces would be named **wlan1**, **wlan2**, etc.

- Ifconfig
  - With this command you can view IP Address and Hardware / MAC address assign to interface

```
# ifconfig eth0 192.168.50.5 netmask 255.255.255.0
```

PING

```
# ping 4.2.2.2

PING 4.2.2.2 (4.2.2.2) 56(84) bytes of data.
64 bytes from 4.2.2.2: icmp_seq=1 ttl=44 time=203 ms
64 bytes from 4.2.2.2: icmp_seq=2 ttl=44 time=201 ms
64 bytes from 4.2.2.2: icmp_seq=3 ttl=44 time=201 ms

OR

# ping www.tecmint.com

PING tecmint.com (50.116.66.136) 56(84) bytes of data.
64 bytes from 50.116.66.136: icmp_seq=1 ttl=47 time=284 ms
64 bytes from 50.116.66.136: icmp_seq=2 ttl=47 time=287 ms
64 bytes from 50.116.66.136: icmp_seq=3 ttl=47 time=285 ms
```

- PING
  - to test connectivity between two nodes. Ping use ICMP (Internet Control Message Protocol) to communicate to other devices.
  - ICMP – network layer protocol, used to send error messages and optional information including success or failure when communicating with another device.
  - Types of ICMP messages:
    - 1. Eco Request and Eco Reply message – This type of message is used by PING utility
    - 2. Time exceeded in transit message – Time to Live (TTL) expired in transit.
    - 3. Destination Unreachable message – Destination host unreachable.

- Route
  - shows and allows manipulation of IP routing table.

```
# route

Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
192.168.50.0    *               255.255.255.0   U     0      0        0 eth0
link-local      *               255.255.0.0     U     1002   0        0 eth0
default         192.168.50.1    0.0.0.0         UG    0      0        0 eth0
```

Destination – The destination network or destination host
Gateway – Gateway address or * if not set
Genmask – The netmask for destination network; 255.255.255.0 for a host destination and 0.0.0.0 for default route
U – Up, G – gateway
Metric – Distance in Hops, Iface – Interface to which the packets for this route will be sent

- Route

Adding, deleting routes and default Gateway with following commands.

Route Adding

```
# route add -net 10.10.10.0/24 gw 192.168.0.1
```

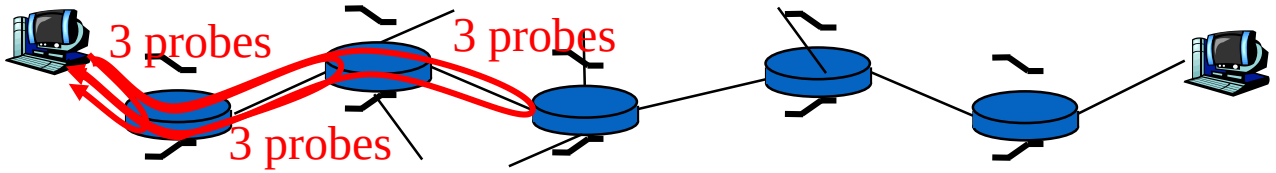
Route Deleting

```
# route del -net 10.10.10.0/24 gw 192.168.0.1
```

Adding default Gateway

```
# route add default gw 192.168.0.1
```

- Traceroute
  - shows number of hops taken to reach destination also determine packets traveling path.
    - **Traceroute program:** provides delay measurement from source to router along end-end Internet path towards destination. For all *i:*
      - sends three packets that will reach router *i* on path towards destination
      - router *i* will return packets to sender
      - sender times interval between transmission and reply.



Three delay measurements from gaia.cs.umass.edu to cs-gw.cs.umass.edu

```
1  cs-gw (128.119.240.254)  1 ms  1 ms  2 ms
2  border1-rt-fa5-1-0.gw.umass.edu (128.119.3.145)  1 ms  1 ms  2 ms
3  cht-vbns.gw.umass.edu (128.119.3.130)  6 ms 5 ms 5 ms
4  jn1-at1-0-0-19.wor.vbns.net (204.147.132.129)  16 ms 11 ms 13 ms
5  jn1-so7-0-0-0.wae.vbns.net (204.147.136.136)  21 ms 18 ms 18 ms
6  abilene-vbns.abilene.ucaid.edu (198.32.11.9)  22 ms  18 ms  22 ms
7  nycm-wash.abilene.ucaid.edu (198.32.8.46)  22 ms  22 ms  22 ms
8  62.40.103.253 (62.40.103.253)  104 ms 109 ms 106 ms
9  de2-1.de1.de.geant.net (62.40.96.129)  109 ms 102 ms 104 ms
10  de.fr1.fr.geant.net (62.40.96.50)  113 ms 121 ms 114 ms
11  renater-gw.fr1.fr.geant.net (62.40.103.54)  112 ms  114 ms  112 ms
12  nio-n2.cssi.renater.fr (193.51.206.13)  111 ms  114 ms  116 ms
13  nice.cssi.renater.fr (195.220.98.102)  123 ms  125 ms  124 ms
14  r3t2-nice.cssi.renater.fr (195.220.98.110)  126 ms  126 ms  124 ms
15  eurecom-valbonne.r3t2.ft.net (193.48.50.54)  135 ms  128 ms  133 ms
16  194.214.211.25 (194.214.211.25)  126 ms  128 ms  126 ms
17  * * *
18  * * *
19  fantasia.eurecom.fr (193.55.113.142)  132 ms  128 ms  136 ms
```

trans-oceanic link

* means no response (probe lost, router not replying)

- Understanding traceroute output

- ARP
  - ARP (Address Resolution Protocol) is useful to **view** / **add** the contents of the kernel's ARP tables.

```
# arp -e

Address                  HWtype  HWaddress           Flags Mask            Iface
192.168.50.1             ether   00:50:56:c0:00:08   C                     eth0
```

C – Complete,
Incomplete,
Complete and manually set

- How ARP works?

- Systems keep an ARP look-up table where they store information about what IP addresses are associated with what MAC addresses.

- When trying to send a packet to an IP address, the system will first consult this table to see if it already knows the MAC address. If there is a value cached, ARP is not used.

- If the IP address is not found in the ARP table, the system will then send a broadcast packet to the network using the ARP protocol to ask "who has 192.168.1.1".

- DNS
  - The Domain Name System (DNS) is the phonebook of the Internet.
  - When users type domain names such as ‘google.com’ or ‘nytimes.com’ into web browsers, DNS is responsible for finding the correct IP address for those sites.