Network Configuration

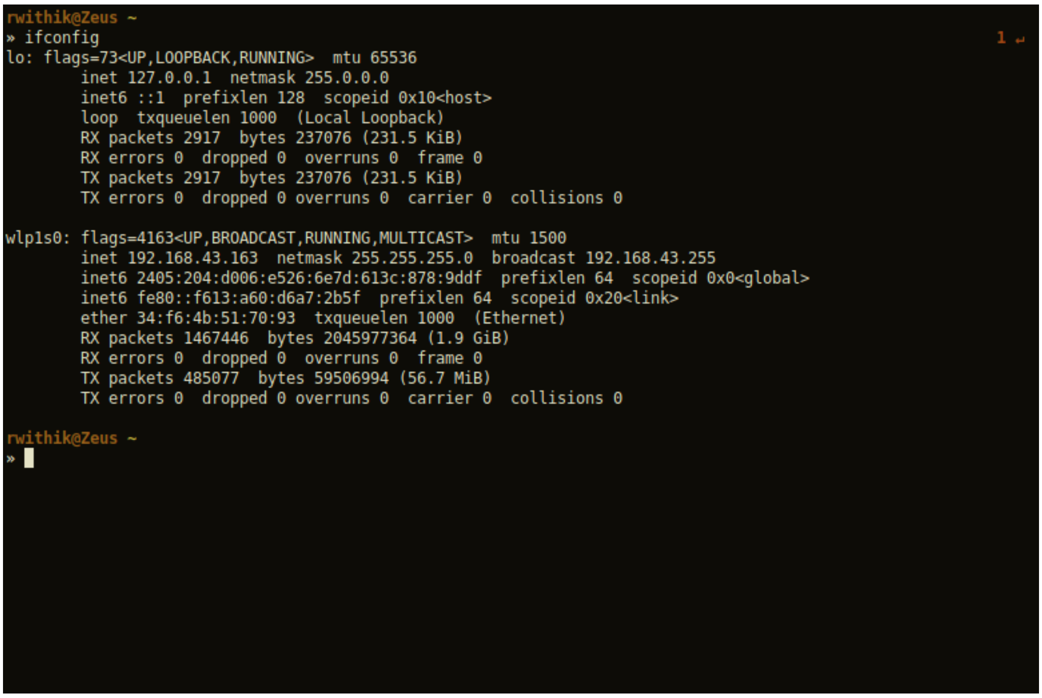
Rwithik Manoj

20-02-2019

About ifconfig

ifconfig, short for “interface configuration” is used to configure, manage and query network interface parameters via command line interface or in system configuration scripts for system/network management in Unix/Linux operating systems.
The command “ifconfig” is used to display current network configuration information, set up an ip address, netmask or broadcast address on a network interface, create an alias for a network interface, set up a hardware address and enable or disable network interfaces.

Using ifconfig with no parameters display the information about the network interfaces that are currently up.

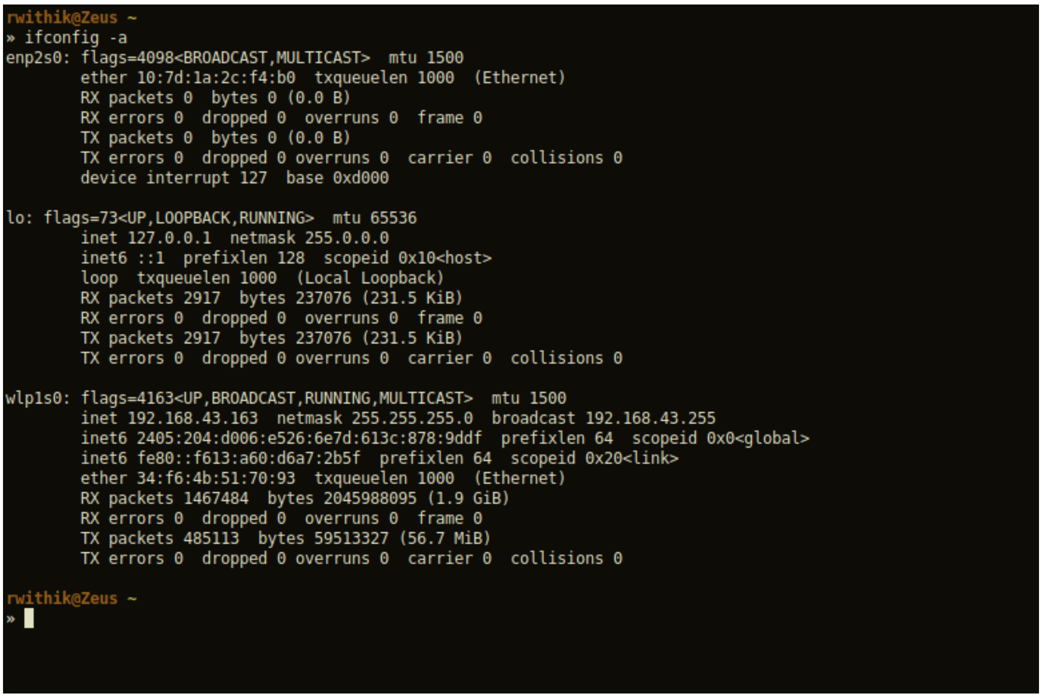


```
rwithik@Zeus ~
» ifconfig                                                                                   1 ↵
lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 2917  bytes 237076 (231.5 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 2917  bytes 237076 (231.5 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

wlp1s0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.43.163  netmask 255.255.255.0  broadcast 192.168.43.255
        inet6 2405:204:d006:e526:6e7d:613c:878:9ddf  prefixlen 64  scopeid 0x0<global>
        inet6 fe80::f613:a60:d6a7:2b5f  prefixlen 64  scopeid 0x20<link>
        ether 34:f6:4b:51:70:93  txqueuelen 1000  (Ethernet)
        RX packets 1467446  bytes 2045977364 (1.9 GiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 485077  bytes 59506994 (56.7 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

rwithik@Zeus ~
» 
```

Using the -a flag displays all the interfaces, even the ones which are down.



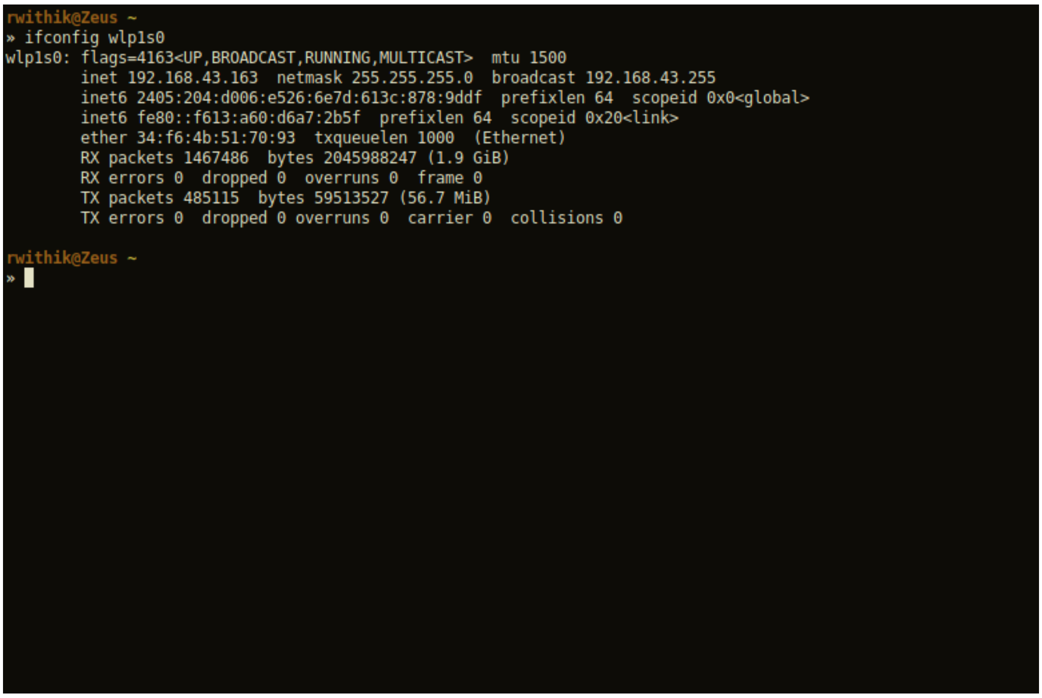
```
rwithik@Zeus ~
» ifconfig -a
enp2s0: flags=4098<BROADCAST,MULTICAST>  mtu 1500
        ether 10:7d:1a:2c:f4:b0  txqueuelen 1000  (Ethernet)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
        device interrupt 127  base 0xd000

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 2917  bytes 237076 (231.5 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 2917  bytes 237076 (231.5 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

wlp1s0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.43.163  netmask 255.255.255.0  broadcast 192.168.43.255
        inet6 2405:204:d006:e526:6e7d:613c:878:9ddf  prefixlen 64  scopeid 0x0<global>
        inet6 fe80::f613:a60:d6a7:2b5f  prefixlen 64  scopeid 0x20<link>
        ether 34:f6:4b:51:70:93  txqueuelen 1000  (Ethernet)
        RX packets 1467484  bytes 2045988095 (1.9 GiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 485113  bytes 59513327 (56.7 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

rwithik@Zeus ~
»
```

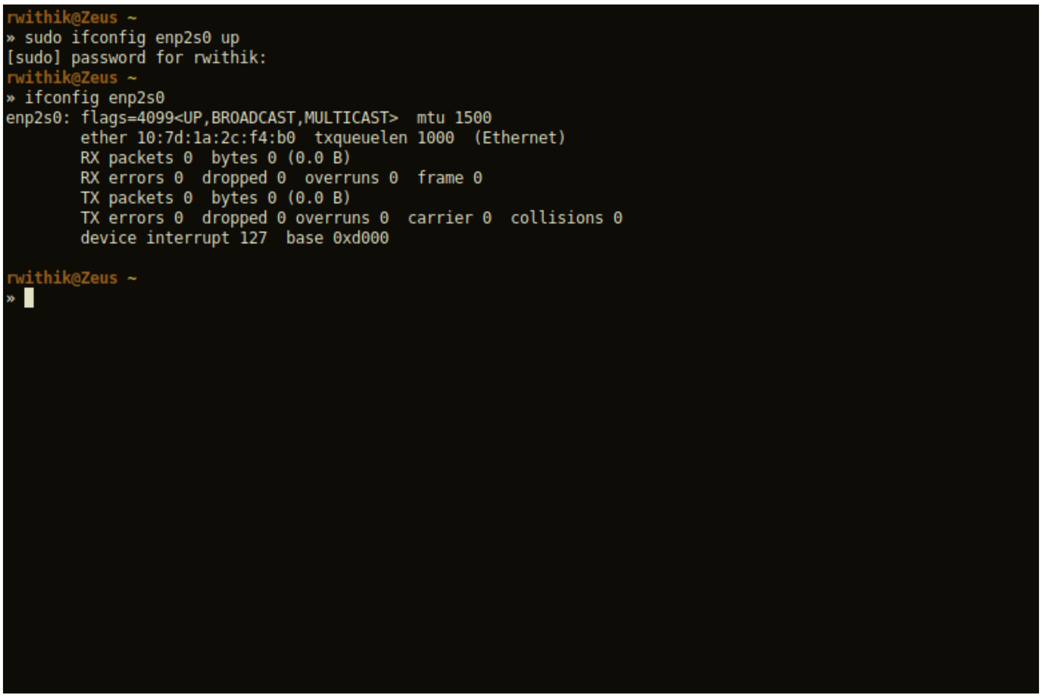
Using ifconfig [INTERFACE NAME] will display the information about the mentioned interface.



```
rwithik@Zeus ~
» ifconfig wlp1s0
wlp1s0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.43.163  netmask 255.255.255.0  broadcast 192.168.43.255
        inet6 2405:204:d006:e526:6e7d:613c:878:9ddf  prefixlen 64  scopeid 0x0<global>
        inet6 fe80::f613:a60:d6a7:2b5f  prefixlen 64  scopeid 0x20<link>
        ether 34:f6:4b:51:70:93  txqueuelen 1000  (Ethernet)
        RX packets 1467486  bytes 2045988247 (1.9 GiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 485115  bytes 59513527 (56.7 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

rwithik@Zeus ~
»
```

Disabling and enabling interfaces with ifconfig.
Syntax: ifconfig [INTERFACE] [up/down]



```
rwithik@Zeus ~
» sudo ifconfig enp2s0 up
[sudo] password for rwithik:
rwithik@Zeus ~
» ifconfig enp2s0
enp2s0: flags=4099<UP,BROADCAST,MULTICAST>  mtu 1500
        ether 10:7d:1a:2c:f4:b0  txqueuelen 1000  (Ethernet)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
        device interrupt 127  base 0xd000

rwithik@Zeus ~
»
```

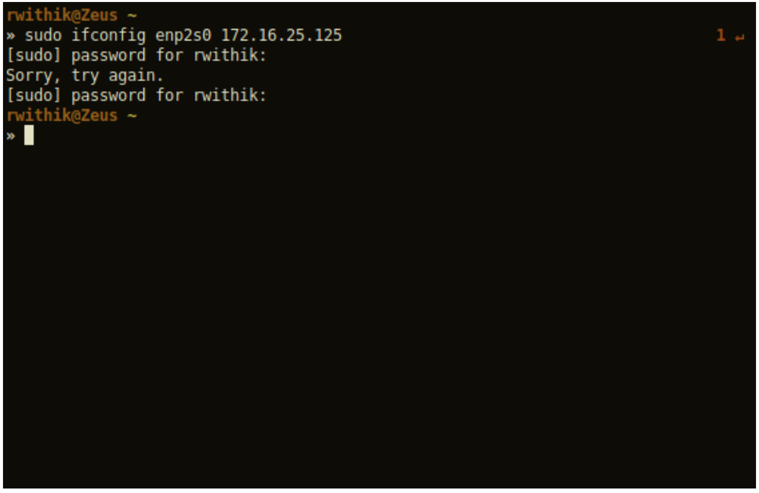
What is a gateway?

A gateway is a network node that connects two networks using different protocols together. The most common gateway is the router. It connect home networks to the internet.
The gateway can be set using the ip route or ip r command.
Syntax: ip route add default via [GATEWAY] dev [INTERFACE]
Example: ip route add default via 192.168.0.254 dev eth0, assuming 192.168.0.254 is the ip of your gateway.

What is a DNS

DNS, or Domain Name Server, translates the domain names to IP addresses, so that the browser can interact with them. Each device connected to the Internet has a unique IP address which other machines use to find the device. DNS servers allows us to simply type the domain as example.com, and be taken to the website instead of typing the IP address of the domain.

Your DNS information is stored in \etc\resolve.conf

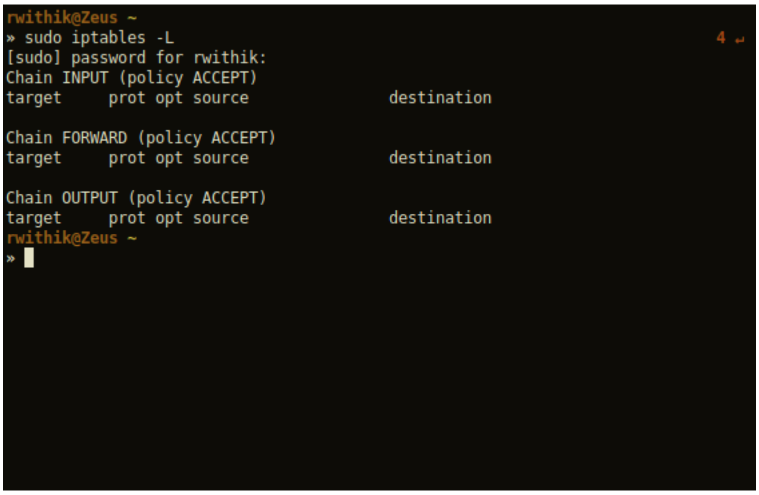


```
rwithik@Zeus ~
» sudo ifconfig enp2s0 172.16.25.125                                   1 ↵
[sudo] password for rwithik:
Sorry, try again.
[sudo] password for rwithik:
rwithik@Zeus ~
» 
```

Just edit this file to set a custom DNS.

About iptables

Iptables is a firewall tool include in the Linux netfilter framework. A firewall is a network security system that monitors and controls on the basis of predetermined security rules incoming and outgoing network traffic. Use iptables -L to list the current rules.



```
rwithik@Zeus ~
» sudo iptables -L                                                            4 ↵
[sudo] password for rwithik:
Chain INPUT (policy ACCEPT)
target     prot opt source               destination

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
rwithik@Zeus ~
»
```

There are two policies- ACCEPT and DENY. ACCEPT allows packages to be received from the mentioned IP addresses. And DROP blocks them.
For Example, if the default policy of INPUT is DROP, iptables blocks all incoming packages.
To allow all packages from your LAN, run this command to add rule to your iptables.
iptables -A INPUT -s 192.168.100.0/24 -j ACCEPT