COMPUTER NETWORKS (CS212) LAB 1

Reference to assignment 1

Agenda

1. Network Utilities or Commands
2. Network Configuration Files
3. Examples on networking tools and files

System Requirements

We will be using linux platform during the entire lab sessions.

Preferably **Ubuntu**

If you are using windows,please ensure to have one of the following :

1. Partition the space and have linux operating system.
2. Install the virtualbox and have ubuntu

Network Utilities Or Commands

1. Ifconfig
2. ping
3. traceroute
4. route
5. arp
6. ssh
7. ftp
8. smtp

Network utilities are basic software tools designed for analyzing and configuring various aspects of computer networks.

Network utilities help you keep your network functioning properly by allowing you to check the various aspects of your network, such as connections between devices, packet loss, and latency between connections. If a network issue arises, a network utility can help you pinpoint the problem

Network Configuration Files

1. /etc/hostname
2. /etc/hosts
3. /etc/network/interfaces
4. /etc/resolv.conf
5. /etc/protocols
6. /etc/services

There are many files under Linux where you can configure - define your Linux network.

The Linux network is configured by settings that are specified in configuration files that you can find in the *\/etc* directory or in one of its subdirectories.

Examples On Network Utilities Or Commands

MAC (Media Access Control) address

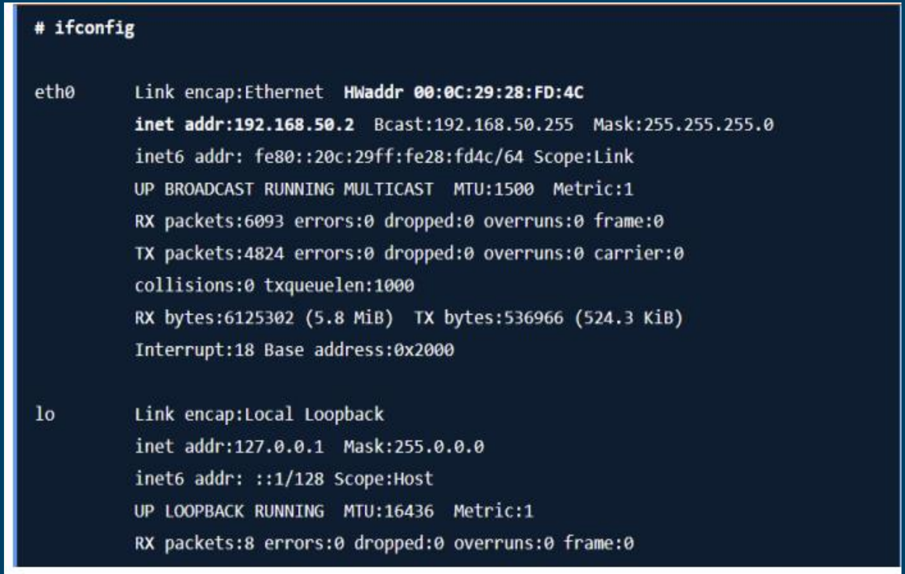
A MAC (or Machine Access Control) address is best thought of as kind of serial number assigned to every network adapter. No two anywhere should have the same MAC address.

IP (Internet Protocol) address

An IP address is assigned to every device on a network, so that device can be located on that network.

1. ifconfig

- interface configurator (ifconfig) is use to initialize an interface, assign IP Address to interface and enable or disable interface on demand.
- With this command you can view IP Address and Hardware / MAC address assign to interface



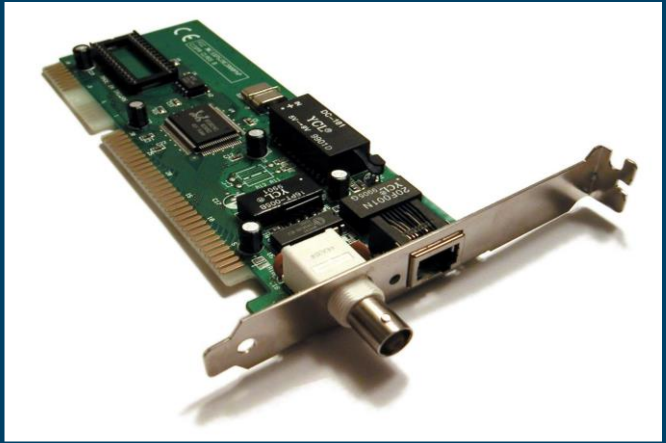
```
# ifconfig

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
```

ip addr

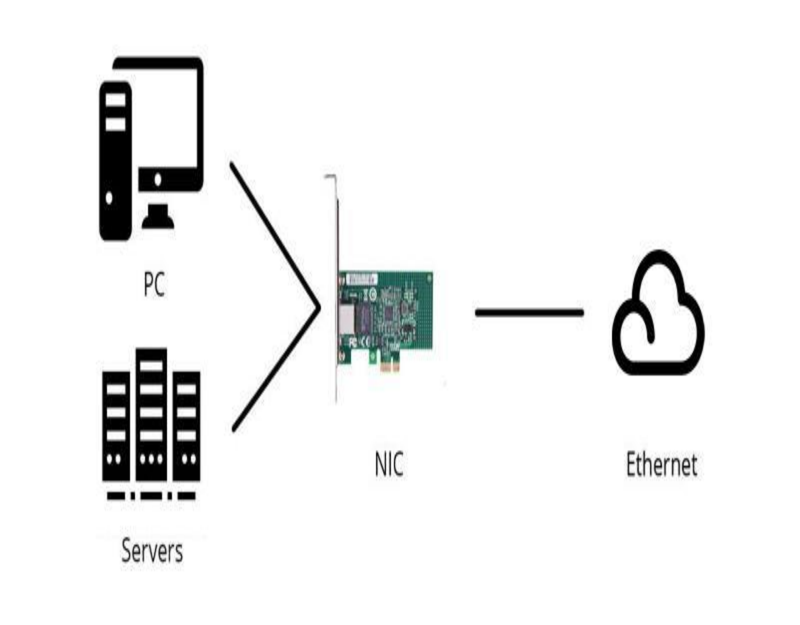
- ifconfig is deprecated in the latest versions of linux platforms.So ip addr command can be used as a replacement for the same.

Network Interface:

- A network interface will usually have some form of network address (IP and MAC address, for instance)



Network Interface (Contd.)



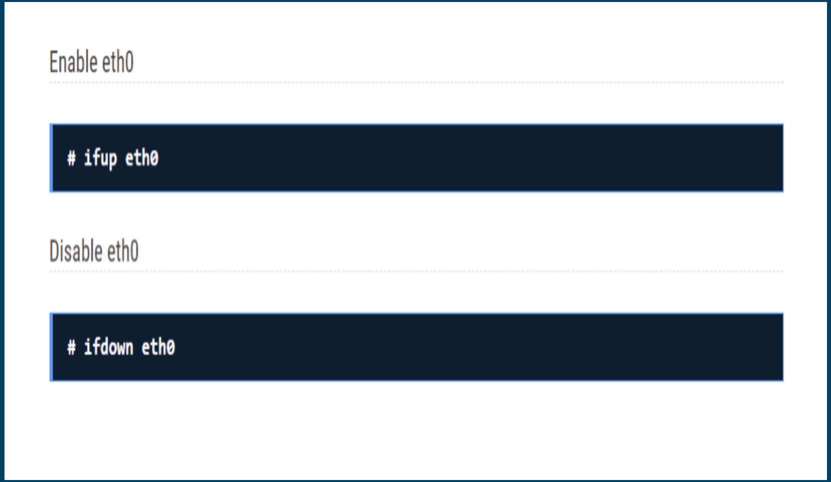
One of the ways to access the internet is to connect a LAN cable(Ethernet Cable) to our computer. What happens when we connect this LAN cable to our computer? This LAN cable connects to a hardware device already present in our computer called **Network Interface card**. So, any computer in order to connect to the internet needs a Network Interface Card(NIC). These days almost all computers have built-in NIC.

Network Interface Card is a hardware device that is installed on the computer so that it can be connected to the internet. It is also called **Ethernet Card** or **Network Adapter.** Every NIC has a 48-bit unique serial number called a MAC address which is stored in ROM carried on the card. Every computer must have **at least one NIC** if it wants to connect to the internet.

Network Interface (Contd.)

- 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.

Enable/Disable interface



Enable eth0

```
# ifup eth0
```

Disable eth0

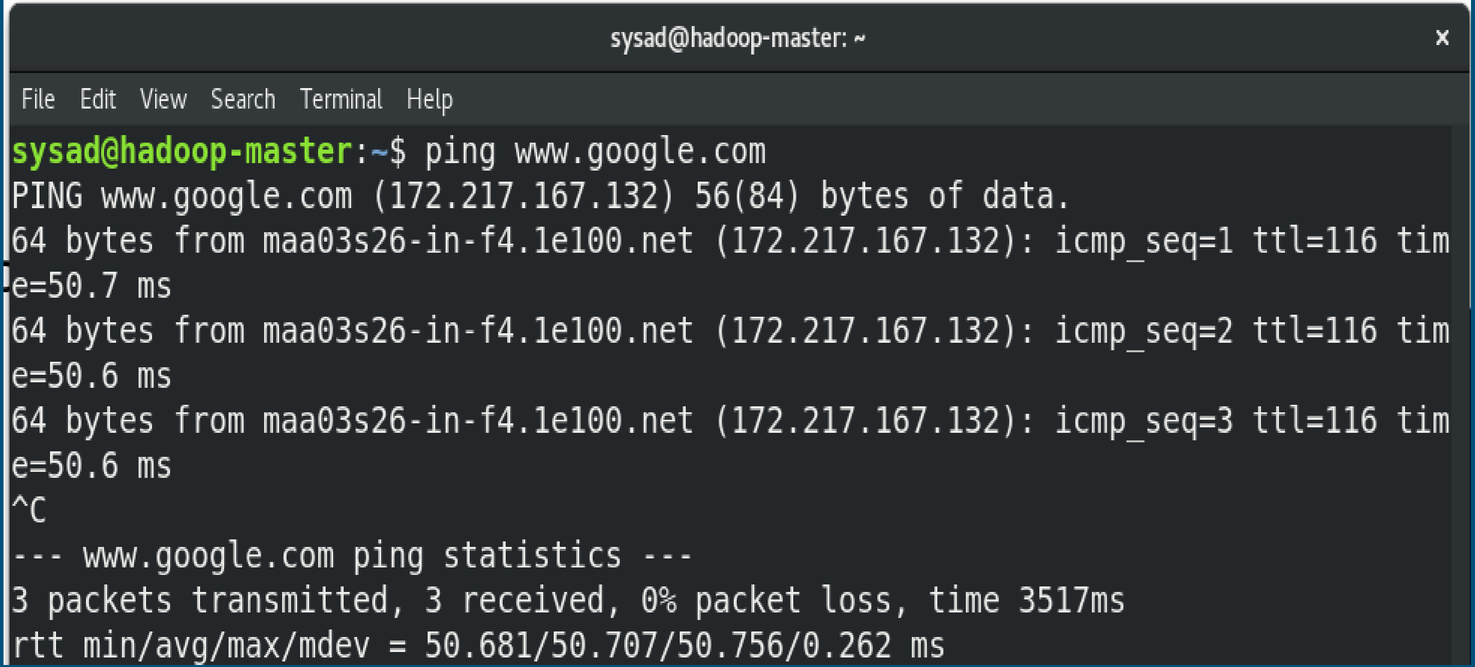
```
# ifdown eth0
```

2. ping

A ping is a Command Prompt command that can be used to test a connection between one computer and another.

Ping measures the round-trip time for messages sent from the originating host to a destination computer that are echoed back to the source.

Round-trip time (RTT) is the duration in milliseconds (ms) it takes for a network request to go from a starting point to a destination and back again to the starting point.



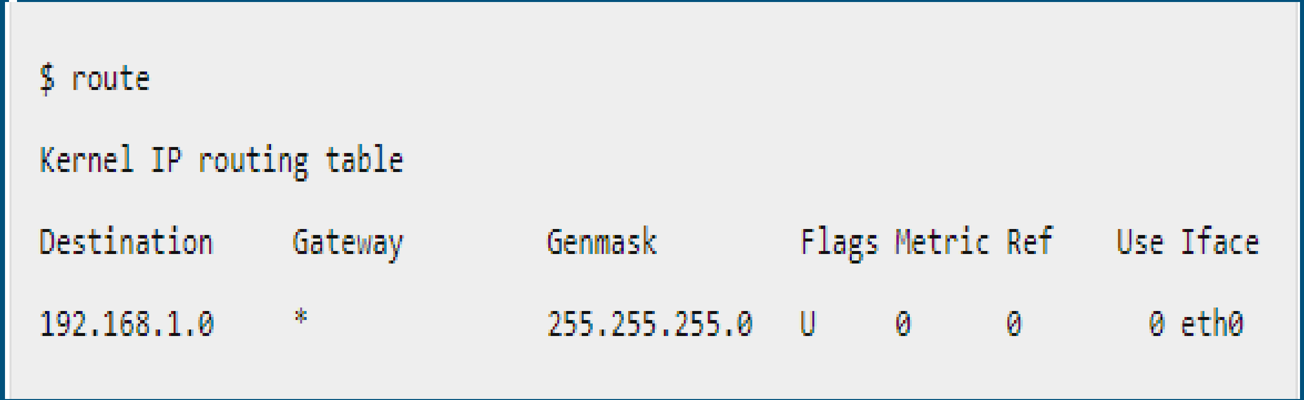
```
sysad@hadoop-master:~$ ping www.google.com
PING www.google.com (172.217.167.132) 56(84) bytes of data.
64 bytes from maa03s26-in-f4.1e100.net (172.217.167.132): icmp_seq=1 ttl=116 tim
e=50.7 ms
64 bytes from maa03s26-in-f4.1e100.net (172.217.167.132): icmp_seq=2 ttl=116 tim
e=50.6 ms
64 bytes from maa03s26-in-f4.1e100.net (172.217.167.132): icmp_seq=3 ttl=116 tim
e=50.6 ms
^C
--- www.google.com ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 3517ms
rtt min/avg/max/mdev = 50.681/50.707/50.756/0.262 ms
```

The terminal output includes a summary table that lists the corresponding response time, the packet size as well as the TTL per response packet. In addition, you receive statistical information on sent, received and lost packets, including packet loss in percentage terms as well as an analysis of the minimum, maximum and average response times.

3. route

shows and allows manipulation of IP routing table.

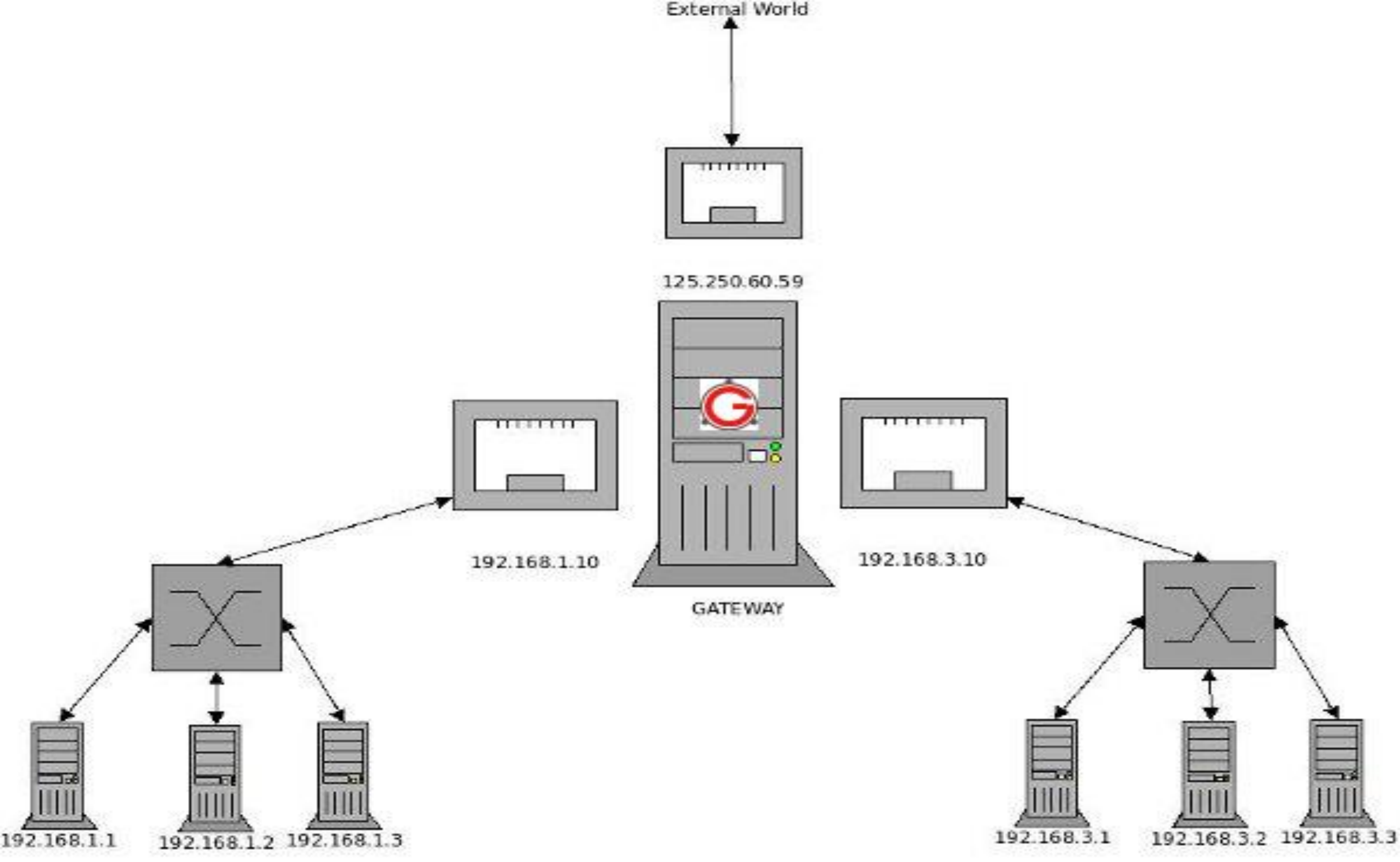
A routing table records the paths that packets should take to reach every destination that the router is responsible for. Think of train timetables, which train passengers consult to decide which train to catch. Routing tables are like that, but for network paths rather than trains.



```
$ route

Kernel IP routing table

Destination     Gateway         Genmask         Flags Metric Ref    Use Iface

192.168.1.0     *               255.255.255.0   U     0      0        0 eth0
```

In this example, the ip-address of the system where the route command is being executed is 192.168.1.157
The above command shows that if the destination is within the network range 192.168.1.0 – 192.168.1.255, then the gateway is *, which is 0.0.0.0.

When packets are sent within this IP range, then the MAC address of the destination is found through ARP Protocol and the packet will be sent to the MAC address.In order to send packets to destination which is not within this ip range, the packets will be forwarded to a default gateway, which decides further routing for that packet.


External World
125.250.60.59
192.168.1.10
192.168.3.10
GATEWAY
192.168.1.1
192.168.1.2
192.168.1.3
192.168.3.1
192.168.3.2
192.168.3.3

In the diagram, we have 2 individual networks (192.168.1.0 and 192.168.3.0, with subnet mask of 255.255.255.0).We also have a “GATEWAY” machine with 3 network cards. 1st card is connected to 192.168.1.0, 2nd card is connected to 192.168.3.0, and the 3rd card is connected to the external world

Make 192.168.3.* Accessible from 192.168.1.*

Now we need to add a routing entry such that we are able to ping 192.168.3. series ip-addresses from 192.168.1. series. The common point we have is the GATEWAY machine.So, on each machine in 192.168.1.* network a default gateway will be added as shown below.

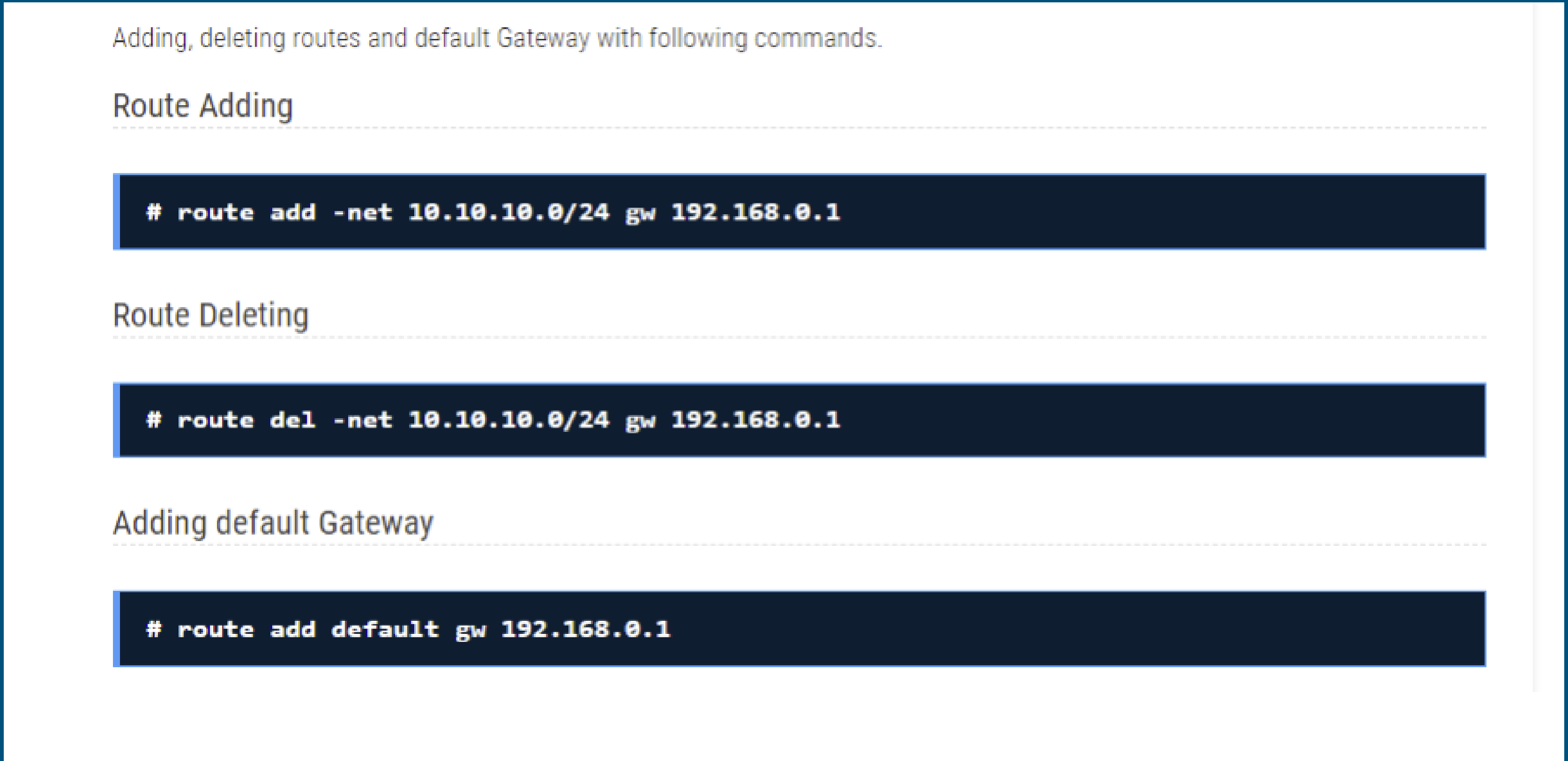
```
  $ route add default gw 192.168.1.10
```

Now when 192.168.1.1 pings 192.168.3.1, it will go to the GATEWAY via 192.168.1.10.

In GATEWAY, add the following routing entry.

```
  $ route add -net 192.168.3.0 netmask 255.255.255.0 gw 192.168.3.10
```

Now all the packets addressed to 192.168.3.* network will be forwarded via the 192.168.3.10 interface, which then delivers the packets to the addressed machine.



Adding, deleting routes and default Gateway with following commands.

Route Adding

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

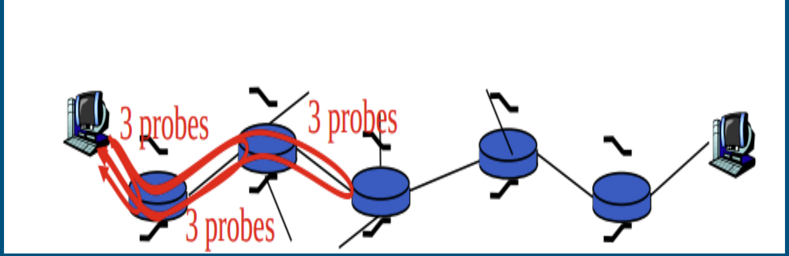
Route Deleting

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

Adding default Gateway

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

4. Traceroute



traceroute command in Linux prints the route that a packet takes to reach the host.

Traceroute is a useful tool for diagnosing network problems, most often speed issues. For example, if your website is slow to load pages then you might use Traceroute to discover the cause. Broadband customers might also use Traceroute if they are unable to connect to certain websites or their connection to the Internet is slow.

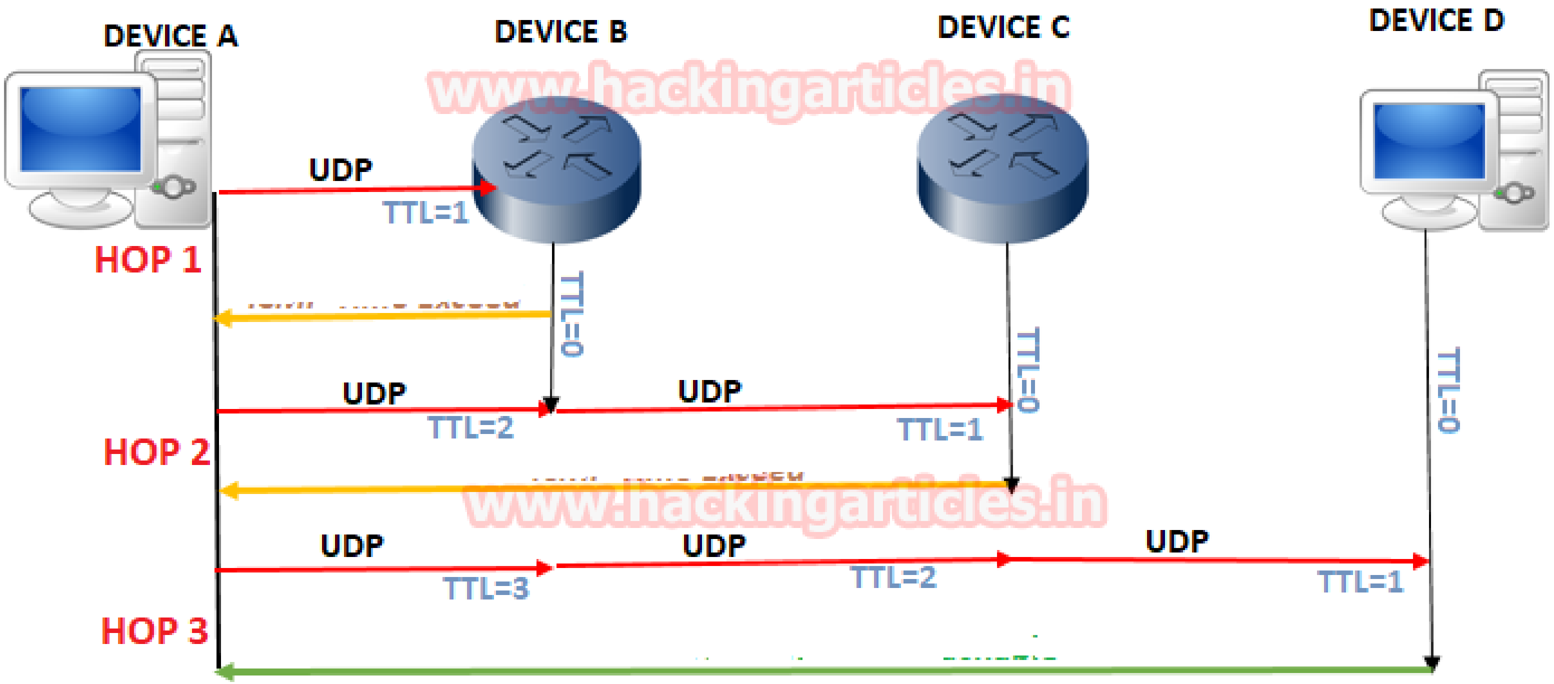
BASICS

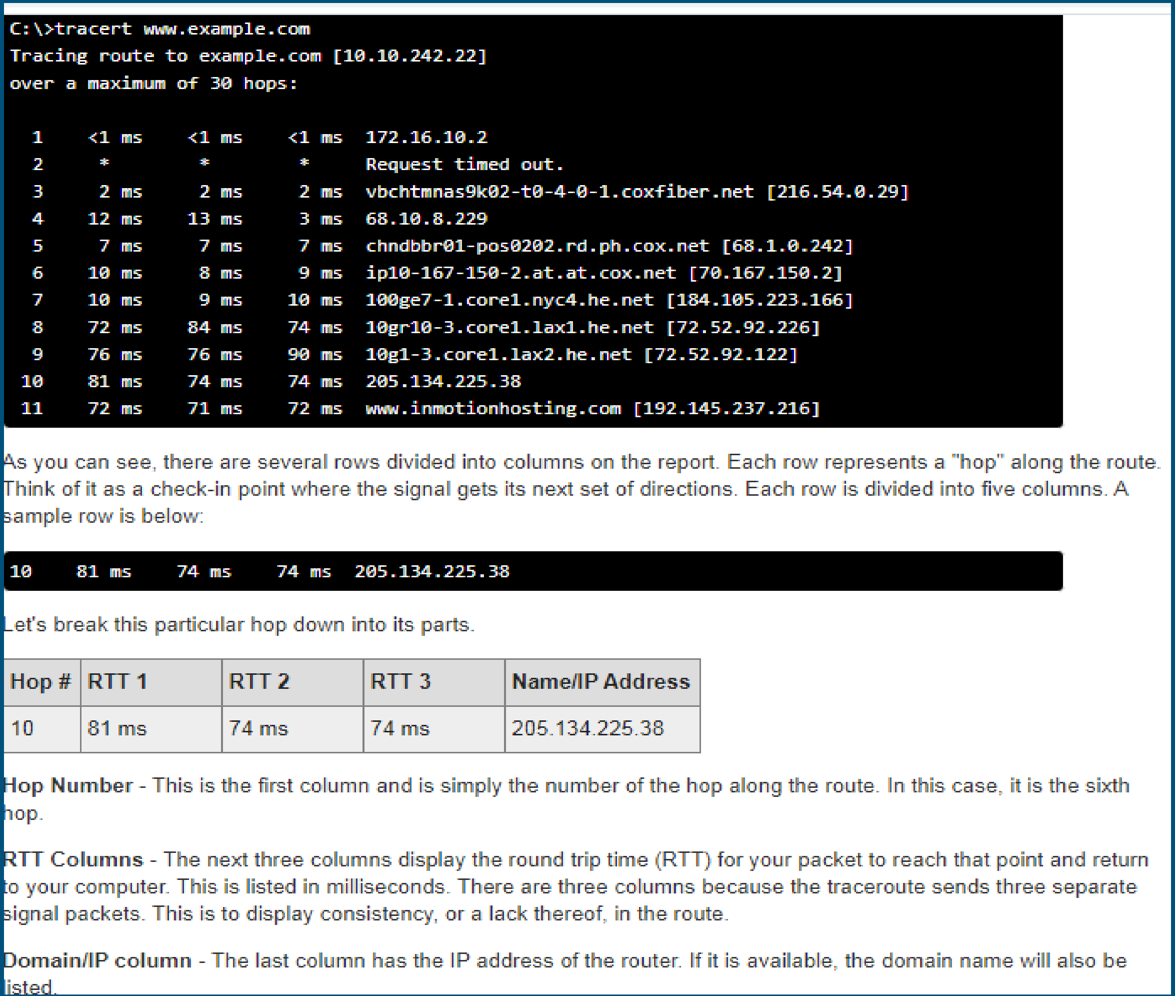
Each IP packet that you send on the internet has got a field called as TTL. TTL stands for Time To Live.

TTL is not measured by the no of seconds but the no of hops. Its the maximum number of hops that a packet can travel through across the internet, before its discarded.

Hops are nothing but the computers, routers, or any devices that comes in between the source and the destination.

Working of Traceroute





```
C:\>tracert www.example.com
Tracing route to example.com [10.10.242.22]
over a maximum of 30 hops:

  1    <1 ms    <1 ms    <1 ms  172.16.10.2
  2     *        *        *     Request timed out.
  3     2 ms     2 ms     2 ms  vbchtmnas9k02-t0-4-0-1.coxfiber.net [216.54.0.29]
  4    12 ms    13 ms     3 ms  68.10.8.229
  5     7 ms     7 ms     7 ms  chndbbr01-pos0202.rd.ph.cox.net [68.1.0.242]
  6    10 ms     8 ms     9 ms  ip10-167-150-2.at.at.cox.net [70.167.150.2]
  7    10 ms     9 ms    10 ms  100ge7-1.core1.nyc4.he.net [184.105.223.166]
  8    72 ms    84 ms    74 ms  10gr10-3.core1.lax1.he.net [72.52.92.226]
  9    76 ms    76 ms    90 ms  10g1-3.core1.lax2.he.net [72.52.92.122]
 10    81 ms    74 ms    74 ms  205.134.225.38
 11    72 ms    71 ms    72 ms  www.inmotionhosting.com [192.145.237.216]
```

As you can see, there are several rows divided into columns on the report. Each row represents a "hop" along the route. Think of it as a check-in point where the signal gets its next set of directions. Each row is divided into five columns. A sample row is below:

```
10    81 ms    74 ms    74 ms  205.134.225.38
```

Let's break this particular hop down into its parts.

Hop #	RTT 1	RTT 2	RTT 3	Name/IP Address
10	81 ms	74 ms	74 ms	205.134.225.38

Hop Number - This is the first column and is simply the number of the hop along the route. In this case, it is the sixth hop.

RTT Columns - The next three columns display the round trip time (RTT) for your packet to reach that point and return to your computer. This is listed in milliseconds. There are three columns because the traceroute sends three separate signal packets. This is to display consistency, or a lack thereof, in the route.

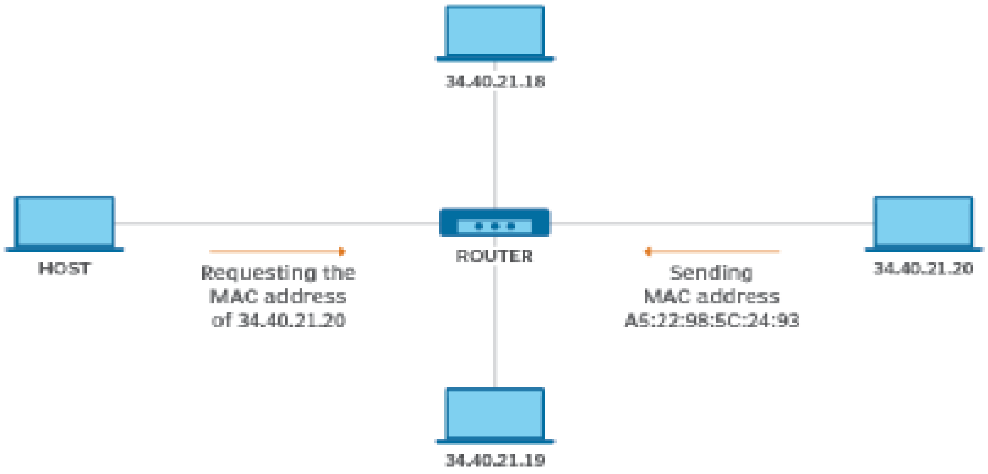
Domain/IP column - The last column has the IP address of the router. If it is available, the domain name will also be listed.

5. ARP

ARP Command is a TCP/IP utility and Microsoft Windows **command** for viewing and modifying the local Address Resolution Protocol (**ARP**) cache, which contains recently resolved MAC addresses of Internet Protocol (IP) hosts on the **network**.

You can use the **arp** command to view and modify the ARP table entries on the local computer.

How address resolution protocol (ARP) works


34.40.21.18
HOST
Requesting the MAC address of 34.40.21.20
ROUTER
Sending MAC address A5:22:98:5C:24:93
34.40.21.20
34.40.21.19

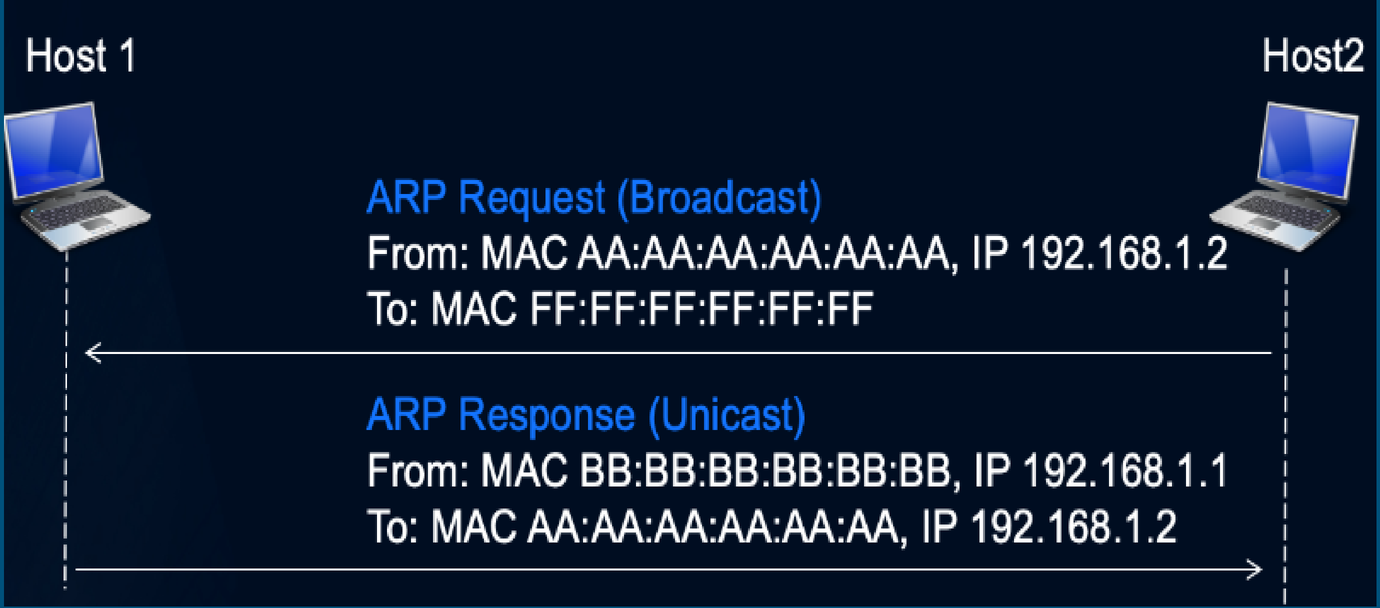
ICONS: MAGLARA/ADOBE STOCK

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".


Host 1
Host2
ARP Request (Broadcast)
From: MAC AA:AA:AA:AA:AA:AA, IP 192.168.1.2
To: MAC FF:FF:FF:FF:FF:FF
ARP Response (Unicast)
From: MAC BB:BB:BB:BB:BB:BB, IP 192.168.1.1
To: MAC AA:AA:AA:AA:AA:AA, IP 192.168.1.2

1. Process begins with caches being empty
2. Host 2 knows that it wants to send a packet to Host 1 (eg Default GW)
3. Host 2 has to send a **broadcast** ARP message (destination FF:FF:FF:FF:FF:FF) requesting an answer for 192.168.1.1.
4. Host 1 responds with its MAC address directly (**unicast**) to Host 2
5. Host 1 and 2 both insert this received information into their ARP caches for future use

6. SSH

SSH is typically **used** to log into a remote machine and execute commands.The ssh command provides a secure encrypted connection between two hosts over an insecure network. This connection can also be used for terminal access, file transfers, and for tunneling other applications

7. FTP

The FTP (**F**ile **T**ransfer **P**rotocol) utility program is commonly used for copying files to and from other computers. These computers may be at the same site or at different sites thousands of miles apart.

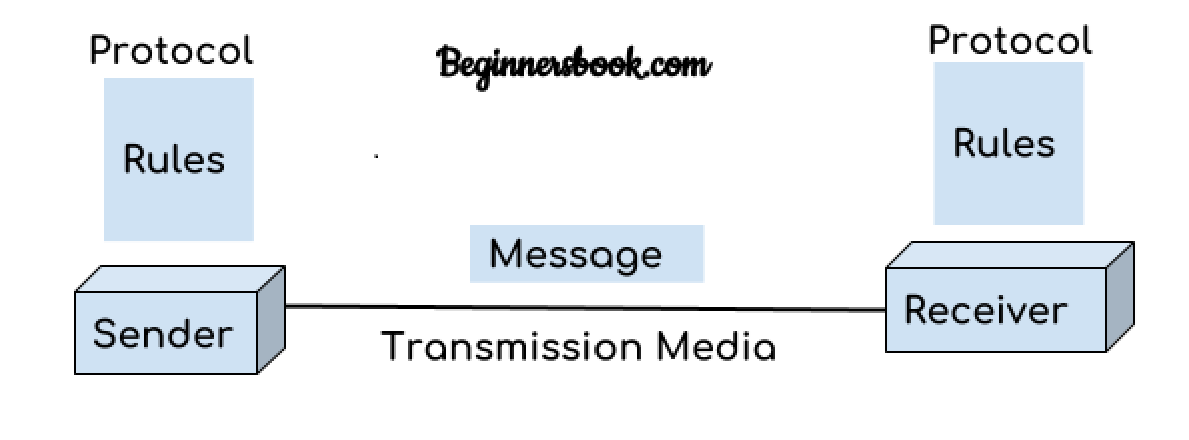
8. SMTP

Simple Mail Transfer Protocol (SMTP) is an Internet standard for sending emails.When you send an email, you are actually sending a bunch of commands to the SMTP server.

IMPORTANT TERMS

Protocols

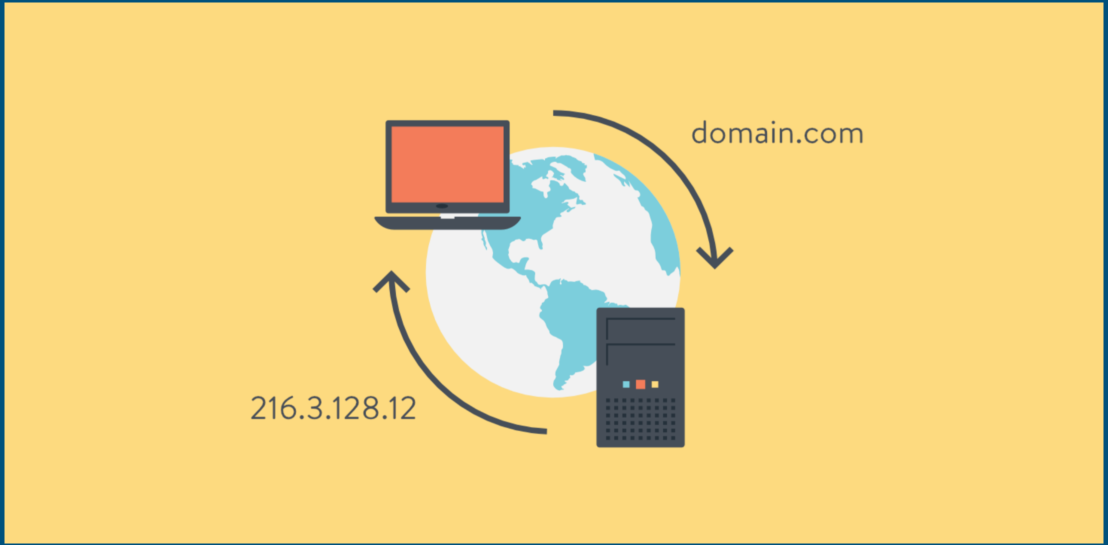
ın networking, a protocol is a set of rules for formatting and processing data. Network protocols are like a common language for computers. The computers within a network may use vastly different software and hardware; however, the use of protocols enables them to communicate with each other regardless.



DNS

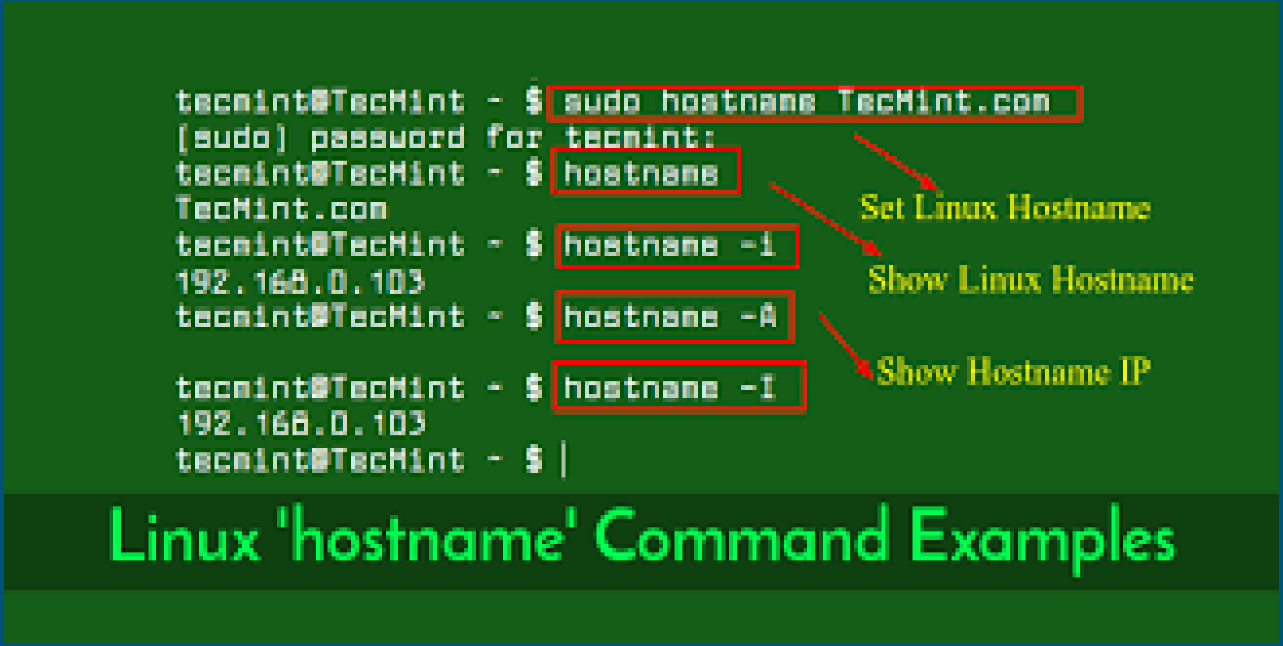
- The Domain Name System (DNS) is the phonebook of the Internet.

- 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., it takes a human-friendly request – a domain name like kinsta.com – and translates it into a computer-friendly server IP address – like 216.3.128.12.



Hostname

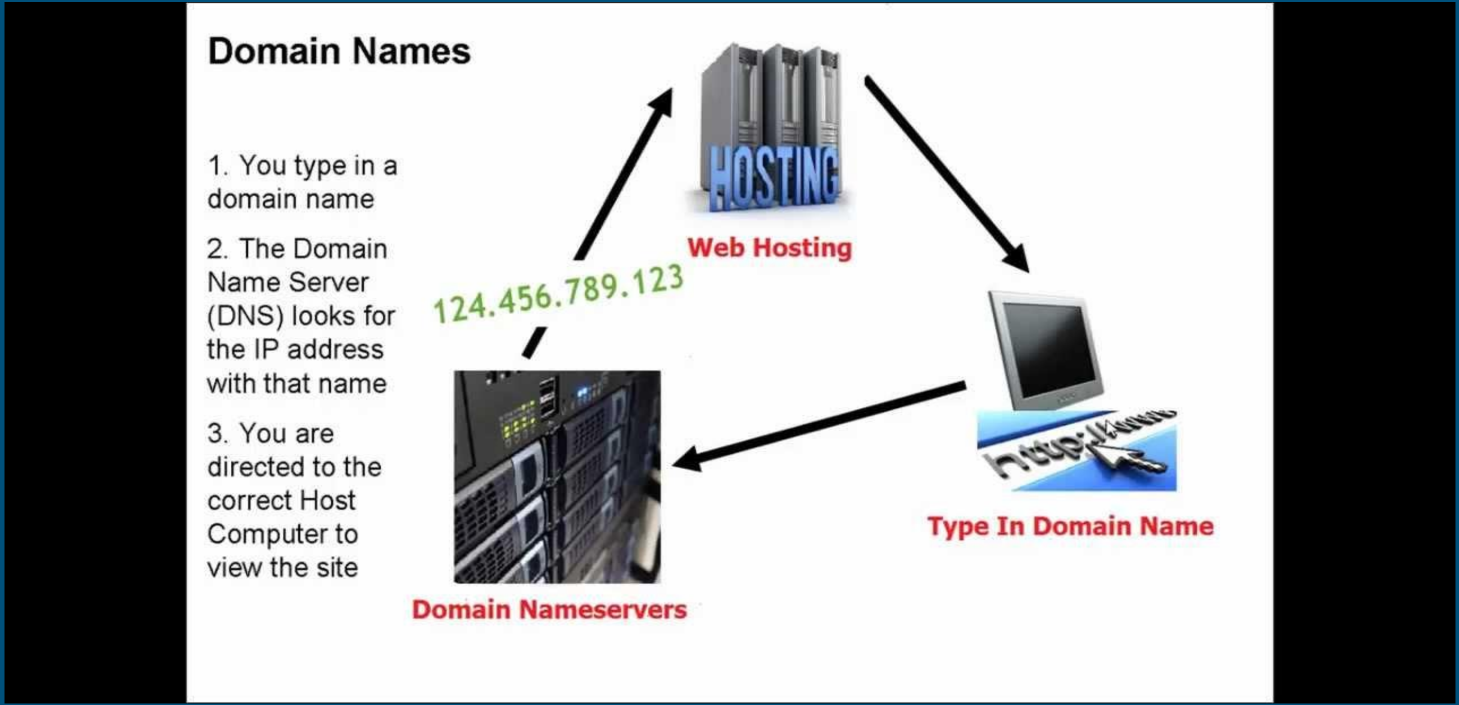
A hostname is a unique name for a computer or network node in a network. Hostnames are specific names or character strings that refer to a host and make it usable for the network and people.



```
tecmint@TecMint ~ $ sudo hostname TecMint.com
[sudo] password for tecmint:
tecmint@TecMint ~ $ hostname
TecMint.com
tecmint@TecMint ~ $ hostname -i
192.168.0.103
tecmint@TecMint ~ $ hostname -A

tecmint@TecMint ~ $ hostname -I
192.168.0.103
tecmint@TecMint ~ $ |
```

Nameserver

A name server is a specialized server on the Internet that handles queries or questions from your local computer, about the location of a domain name’s various services.



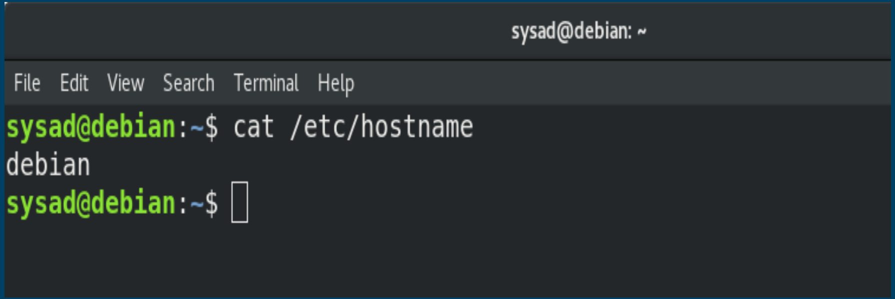
Domain Names

1. You type in a domain name
2. The Domain Name Server (DNS) looks for the IP address with that name
3. You are directed to the correct Host Computer to view the site

Examples On Network Configuration Files

1. /etc/hostname

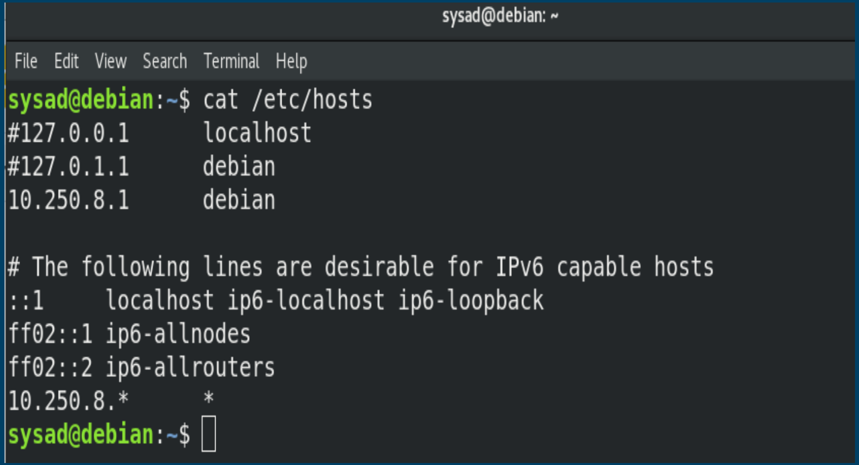
This file stores your system's host name, your system's fully qualified domain name



```
sysad@debian:~$ cat /etc/hostname
debian
sysad@debian:~$ 
```

2. /etc/hosts

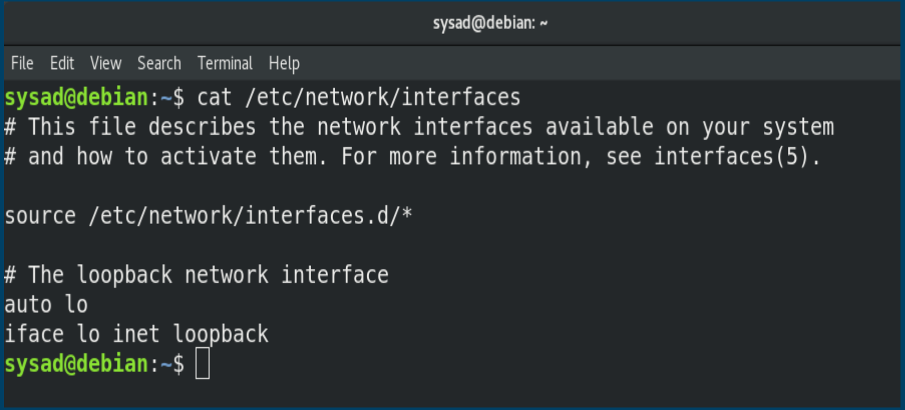
The **/etc/hosts** is an operating system **file** that translate hostnames or domain names to IP addresses



```
sysad@debian:~$ cat /etc/hosts
#127.0.0.1      localhost
#127.0.1.1      debian
10.250.8.1      debian

# The following lines are desirable for IPv6 capable hosts
::1     localhost ip6-localhost ip6-loopback
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
10.250.8.*      *
sysad@debian:~$ 
```

3. /etc/network/interfaces

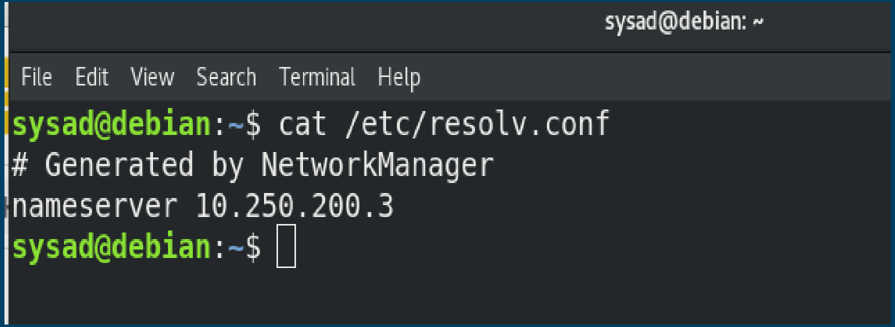
/etc/network/interfaces file contains network interface configuration information for the both Ubuntu and Debian Linux. This is where you configure how your system is connected to the network.



```
sysad@debian:~$ cat /etc/network/interfaces
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

source /etc/network/interfaces.d/*

# The loopback network interface
auto lo
iface lo inet loopback
sysad@debian:~$ 
```

4. /etc/resolv.conf

Lists nameservers that are used by your host for DNS resolution. If you are using `DHCP`, this file is automatically populated with DNS record issued by `DHCP` server.

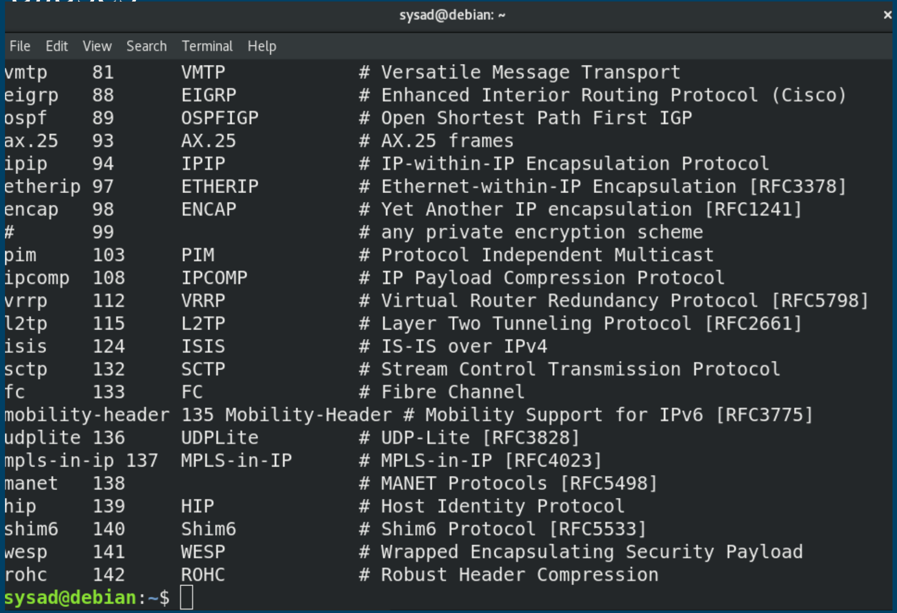


```
sysad@debian:~$ cat /etc/resolv.conf
# Generated by NetworkManager
nameserver 10.250.200.3
sysad@debian:~$ 
```

5. /etc/protocols

The /etc/protocols file contains information regarding the known protocol. For each protocol, a single line should be present with the following information:

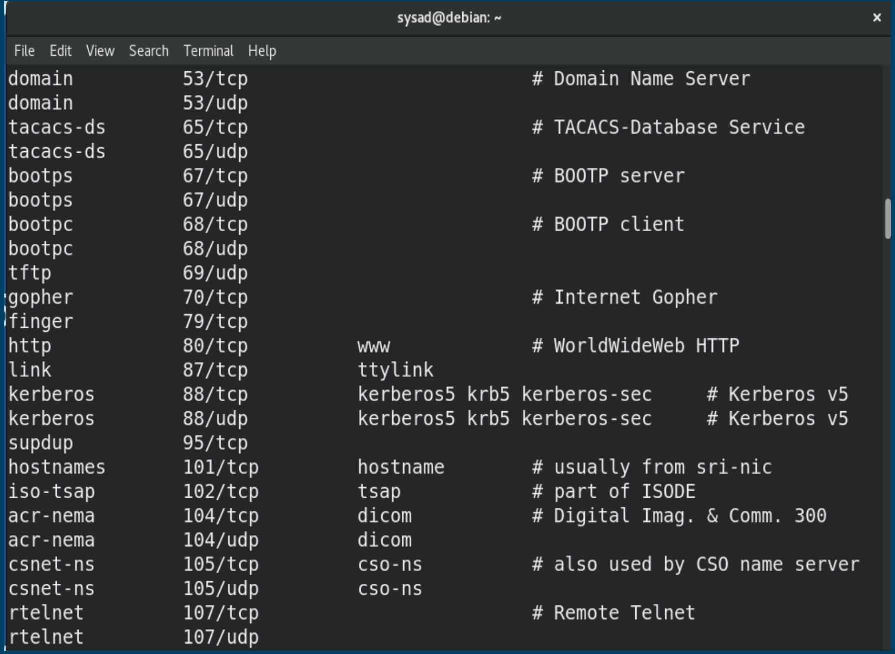
official_protocol_name protocol_number aliases



```
vmtp     81      VMTP            # Versatile Message Transport
eigrp    88      EIGRP           # Enhanced Interior Routing Protocol (Cisco)
ospf     89      OSPFIGP         # Open Shortest Path First IGP
ax.25    93      AX.25           # AX.25 frames
ipip     94      IPIP            # IP-within-IP Encapsulation Protocol
etherip 97       ETHERIP         # Ethernet-within-IP Encapsulation [RFC3378]
encap    98      ENCAP           # Yet Another IP encapsulation [RFC1241]
#        99                      # any private encryption scheme
pim      103     PIM             # Protocol Independent Multicast
ipcomp   108     IPCOMP          # IP Payload Compression Protocol
vrrp     112     VRRP            # Virtual Router Redundancy Protocol [RFC5798]
l2tp     115     L2TP            # Layer Two Tunneling Protocol [RFC2661]
isis     124     ISIS            # IS-IS over IPv4
sctp     132     SCTP            # Stream Control Transmission Protocol
fc       133     FC              # Fibre Channel
mobility-header 135 Mobility-Header # Mobility Support for IPv6 [RFC3775]
udplite 136      UDPLite         # UDP-Lite [RFC3828]
mpls-in-ip 137   MPLS-in-IP      # MPLS-in-IP [RFC4023]
manet    138                     # MANET Protocols [RFC5498]
hip      139     HIP             # Host Identity Protocol
shim6    140     Shim6           # Shim6 Protocol [RFC5533]
wesp     141     WESP            # Wrapped Encapsulating Security Payload
rohc     142     ROHC            # Robust Header Compression
sysad@debian:~$ 
```

6. /etc/services

/etc/services file contains a list of network services and ports mapped to them



```
domain          53/tcp                          # Domain Name Server
domain          53/udp
tacacs-ds       65/tcp                          # TACACS-Database Service
tacacs-ds       65/udp
bootps          67/tcp                          # BOOTP server
bootps          67/udp
bootpc          68/tcp                          # BOOTP client
bootpc          68/udp
tftp            69/udp
gopher          70/tcp                          # Internet Gopher
finger          79/tcp
http            80/tcp          www             # WorldWideWeb HTTP
link            87/tcp          ttylink
kerberos        88/tcp          kerberos5 krb5 kerberos-sec     # Kerberos v5
kerberos        88/udp          kerberos5 krb5 kerberos-sec     # Kerberos v5
supdup          95/tcp
hostnames       101/tcp         hostname        # usually from sri-nic
iso-tsap        102/tcp         tsap            # part of ISODE
acr-nema        104/tcp         dicom           # Digital Imag. & Comm. 300
acr-nema        104/udp         dicom
csnet-ns        105/tcp         cso-ns          # also used by CSO name server
csnet-ns        105/udp         cso-ns
rtelnet         107/tcp                         # Remote Telnet
rtelnet         107/udp
```

THANK YOU