

## EXPERIMENT-2: Network commands and Configuration tools:

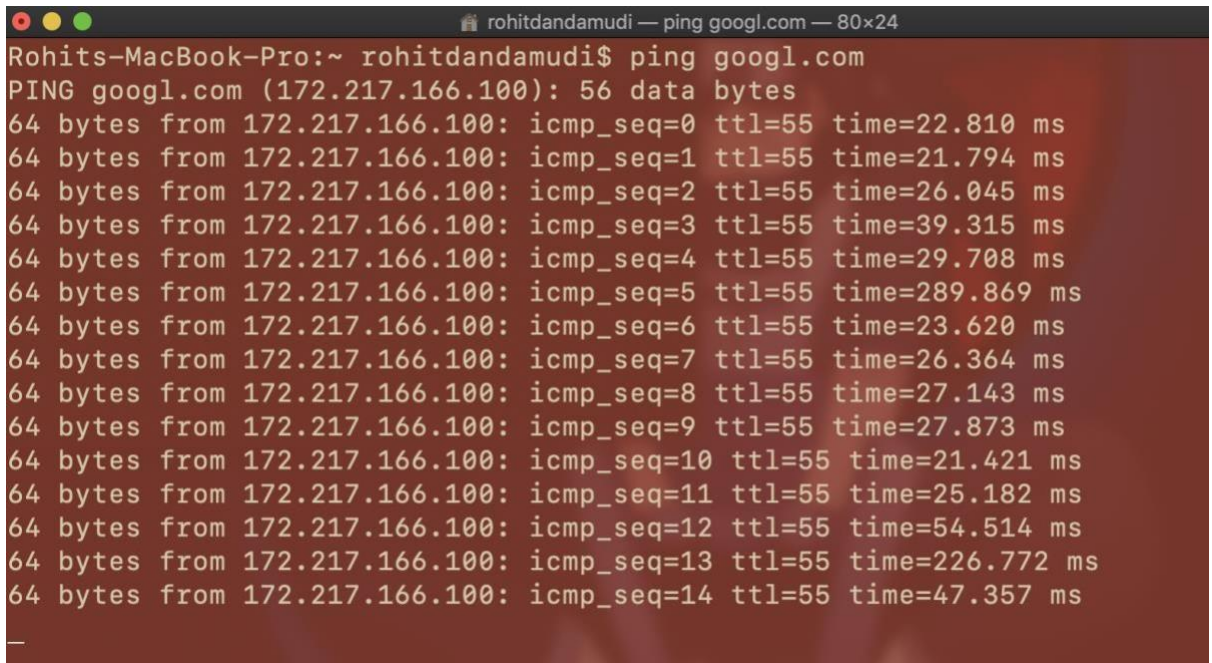
### 1. Ifconfig(Interface configuration)

- Syntax: ifconfig
- ifconfig in short “interface configuration” utility for system/network administration in Unix/Linux operating systems to configure, manage and query network interface parameters via command line interface or in a system configuration scripts.
- The “ifconfig” command is used for displaying current network configuration information, setting up an ip address, netmask or broadcast address to an network interface, creating an alias for network interface, setting up hardware address and enable or disable network interface
- We can many options such as -a for all etc
- Enp1s0 tell ethernet port 1 and socket 0
- UP BROADCAST RUNNING MULTICAST etc are flags that describe the interfaces used

```
rohitdandamudi ~ -bash — 80x24
Last login: Tue Jul 23 15:24:49 on console
Rohits-MacBook-Pro:~ rohitdandamudi$ ifconfig
lo0: flags=8049<UP,LOOPBACK,RUNNING,MULTICAST> mtu 16384
    options=1203<RXCSUM,TXCSUM,TXSTATUS,SW_TIMESTAMP>
    inet 127.0.0.1 netmask 0xff000000
    inet6 ::1 prefixlen 128
    inet6 fe80::1%lo0 prefixlen 64 scopeid 0x1
    nd6 options=201<PERFORMNUD,DAD>
gif0: flags=8010<POINTOPOINT,MULTICAST> mtu 1280
stf0: flags=0<> mtu 1280
XHC0: flags=0<> mtu 0
XHC20: flags=0<> mtu 0
en0: flags=8863<UP,BROADCAST,SMART,RUNNING,SIMPLEX,MULTICAST> mtu 1500
    ether f0:18:98:03:a7:35
    inet6 fe80::1064:5e3:1734:eac0%en0 prefixlen 64 secured scopeid 0x6
    inet6 2402:8100:285a:7021:14f2:78fc:d106:131f prefixlen 64 autoconf secu
red
    inet6 2402:8100:285a:7021:c9fb:de82:cb1b:7804 prefixlen 64 autoconf temp
orary
    inet 192.168.43.213 netmask 0xffffffff broadcast 192.168.43.255
    nd6 options=201<PERFORMNUD,DAD>
    media: autoselect
    status: active
p2p0: flags=8843<UP,BROADCAST,RUNNING,SIMPLEX,MULTICAST> mtu 2304
```

## 2. ping:

- Syntax: ping sitename
- The ping command is a command prompt command used to test the ability of the source computer to reach a specified destination computer. The ping command is usually used as a simple way to verify that a computer can communicate over the network with another computer or network device.
- The ping command operates by sending Internet Control Message Protocol (ICMP) Echo Request messages to the destination computer and waiting for a response. How many of those responses are returned, and how long it takes for them to return, are the two major pieces of information that the ping command

A screenshot of a macOS terminal window. The title bar at the top shows three colored window control buttons (red, yellow, green) on the left, and the text 'rohitdandamudi — ping googl.com — 80x24' on the right. The terminal content shows a user at the 'Rohits-MacBook-Pro:~ rohitdandamudi\$' prompt typing 'ping googl.com'. The output shows a series of 15 ping responses from 172.217.166.100, each with 64 bytes, an icmp\_seq number from 0 to 14, a TTL of 55, and a response time in milliseconds. The response times vary, with the last one being significantly higher (47.357 ms) than the others.

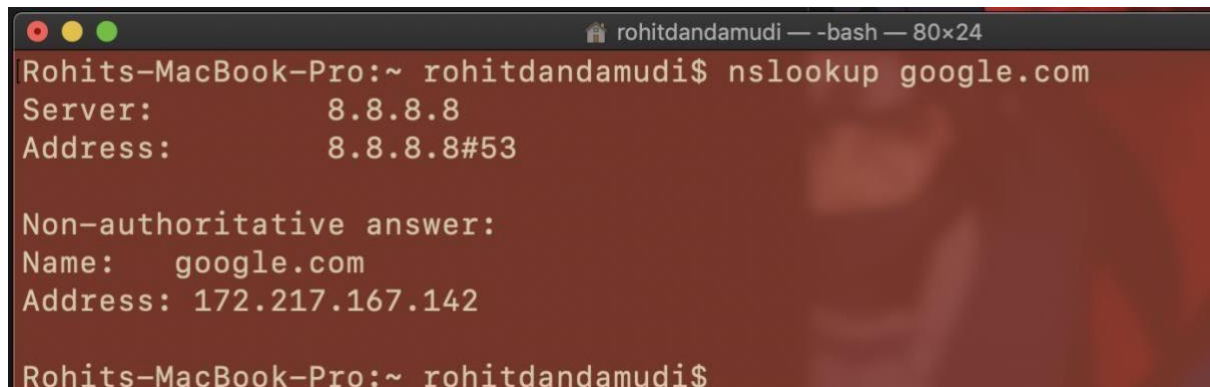
```
Rohits-MacBook-Pro:~ rohitdandamudi$ ping googl.com
PING googl.com (172.217.166.100): 56 data bytes
64 bytes from 172.217.166.100: icmp_seq=0 ttl=55 time=22.810 ms
64 bytes from 172.217.166.100: icmp_seq=1 ttl=55 time=21.794 ms
64 bytes from 172.217.166.100: icmp_seq=2 ttl=55 time=26.045 ms
64 bytes from 172.217.166.100: icmp_seq=3 ttl=55 time=39.315 ms
64 bytes from 172.217.166.100: icmp_seq=4 ttl=55 time=29.708 ms
64 bytes from 172.217.166.100: icmp_seq=5 ttl=55 time=289.869 ms
64 bytes from 172.217.166.100: icmp_seq=6 ttl=55 time=23.620 ms
64 bytes from 172.217.166.100: icmp_seq=7 ttl=55 time=26.364 ms
64 bytes from 172.217.166.100: icmp_seq=8 ttl=55 time=27.143 ms
64 bytes from 172.217.166.100: icmp_seq=9 ttl=55 time=27.873 ms
64 bytes from 172.217.166.100: icmp_seq=10 ttl=55 time=21.421 ms
64 bytes from 172.217.166.100: icmp_seq=11 ttl=55 time=25.182 ms
64 bytes from 172.217.166.100: icmp_seq=12 ttl=55 time=54.514 ms
64 bytes from 172.217.166.100: icmp_seq=13 ttl=55 time=226.772 ms
64 bytes from 172.217.166.100: icmp_seq=14 ttl=55 time=47.357 ms
_
```

provides.

### 3. Nslookup(name server lookup):

- Syntax: nslookup sitename

nslookup is a network administration command-line tool available in many computer operating systems for querying the Domain Name Server(DNS) to obtain domain name or IP address mapping, or other [DNS records](#). The name "nslookup" means "name server lookup".



```

Rohits-MacBook-Pro:~ rohitdandamudi$ nslookup google.com
Server:      8.8.8.8
Address:     8.8.8.8#53

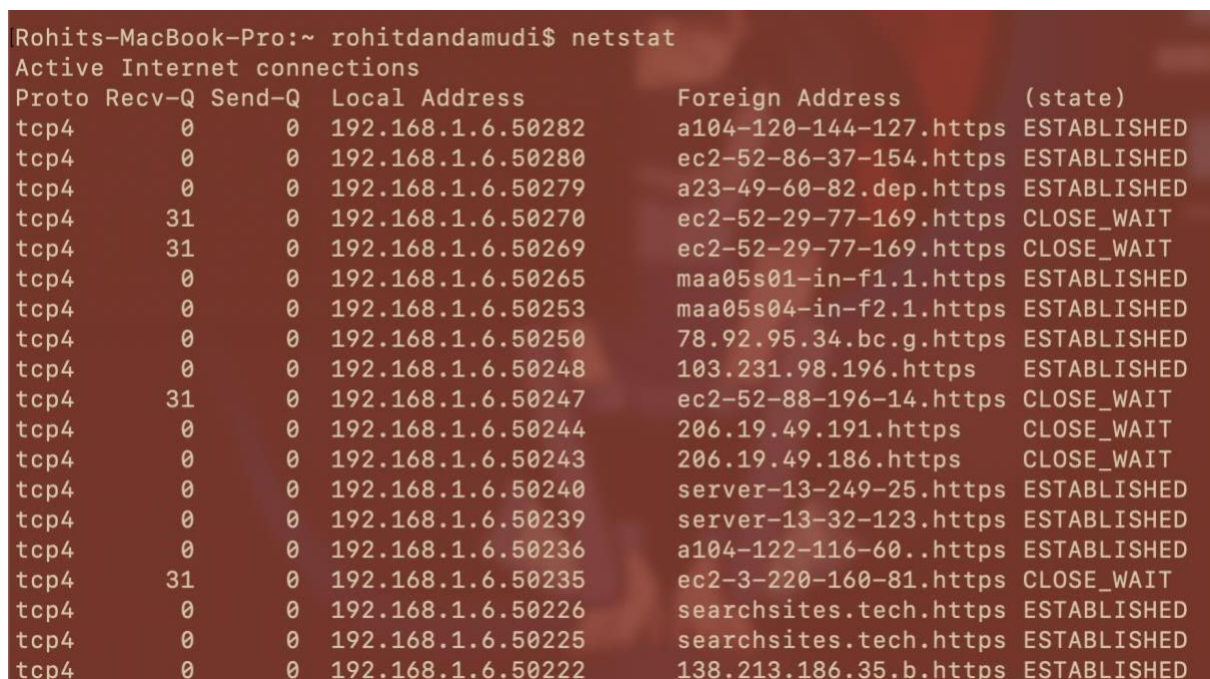
Non-authoritative answer:
Name:   google.com
Address: 172.217.167.142

Rohits-MacBook-Pro:~ rohitdandamudi$
  
```

### 4. Netstat(network statistics):

Netstat is a common command line TCP/IP networking utility available in most other operating systems. Netstat provides information and statistics about protocols in use and current TCP/IP network connections. (The name derives from the words *network* and *statistics*.)

NETSTAT -a -b -e -n -o -p proto -r -s -v interval



```

Rohits-MacBook-Pro:~ rohitdandamudi$ netstat
Active Internet connections
Proto Recv-Q Send-Q Local Address           Foreign Address         (state)
tcp4      0      0 192.168.1.6.50282       a104-120-144-127.https ESTABLISHED
tcp4      0      0 192.168.1.6.50280       ec2-52-86-37-154.https ESTABLISHED
tcp4      0      0 192.168.1.6.50279       a23-49-60-82.dep.https ESTABLISHED
tcp4     31      0 192.168.1.6.50270       ec2-52-29-77-169.https CLOSE_WAIT
tcp4     31      0 192.168.1.6.50269       ec2-52-29-77-169.https CLOSE_WAIT
tcp4      0      0 192.168.1.6.50265       maa05s01-in-f1.1.https ESTABLISHED
tcp4      0      0 192.168.1.6.50253       maa05s04-in-f2.1.https ESTABLISHED
tcp4      0      0 192.168.1.6.50250       78.92.95.34.bc.g.https ESTABLISHED
tcp4      0      0 192.168.1.6.50248       103.231.98.196.https ESTABLISHED
tcp4     31      0 192.168.1.6.50247       ec2-52-88-196-14.https CLOSE_WAIT
tcp4      0      0 192.168.1.6.50244       206.19.49.191.https CLOSE_WAIT
tcp4      0      0 192.168.1.6.50243       206.19.49.186.https CLOSE_WAIT
tcp4      0      0 192.168.1.6.50240       server-13-249-25.https ESTABLISHED
tcp4      0      0 192.168.1.6.50239       server-13-32-123.https ESTABLISHED
tcp4      0      0 192.168.1.6.50236       a104-122-116-60..https ESTABLISHED
tcp4     31      0 192.168.1.6.50235       ec2-3-220-160-81.https CLOSE_WAIT
tcp4      0      0 192.168.1.6.50226       searchsites.tech.https ESTABLISHED
tcp4      0      0 192.168.1.6.50225       searchsites.tech.https ESTABLISHED
tcp4      0      0 192.168.1.6.50222       138.213.186.35.b.https ESTABLISHED
  
```

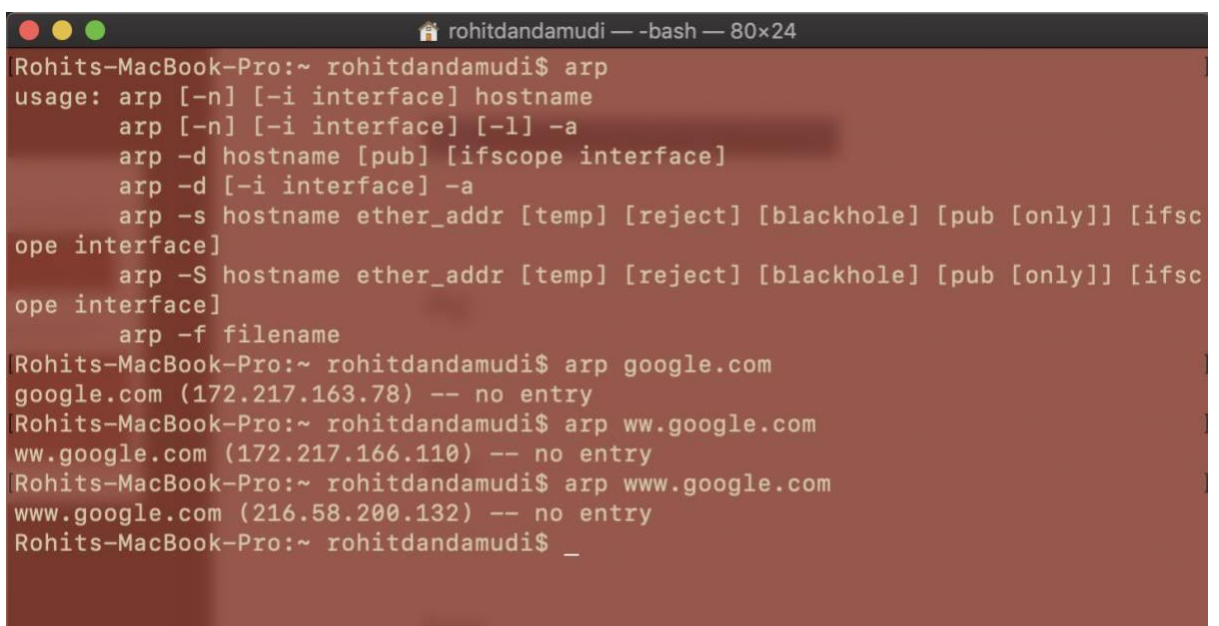


## 5. Nmap(Network Mapper):

- **Nmap** (*Network Mapper*) is a [free and open-source network scanner](#) created by Gordon Lyon (also known by his pseudonym *Fyodor Vaskovich*).<sup>[3]</sup> Nmap is used to discover [hosts](#) and [services](#) on a [computer network](#) by sending [packets](#) and analyzing the responses.
- Nmap provides a number of features for probing computer networks, including host discovery and service and [operating system](#) detection. These features are extensible by [scripts](#) that provide more advanced service detection,<sup>[4]</sup> vulnerability detection,<sup>[4]</sup> and other features. Nmap can adapt to network conditions including [latency](#) and [congestion](#) during a scan.

## 6. arp(Address Resolution Protocol):

- The address resolution protocol (arp) is a protocol used by the [Internet Protocol \(IP\)](#) [\[RFC826\]](#), specifically IPv4, to map [IP network addresses](#) to the hardware addresses used by a data link protocol. The protocol operates below the network layer as a part of the interface between the OSI network and OSI link layer. It is used when [IPv4 is used over Ethernet](#).
- The term address resolution refers to the process of finding an address of a computer in a network. The address is "resolved" using a protocol in which a piece of information is sent by a client process executing on the local computer to a server process executing on a remote computer. The information received by the server allows the server to uniquely identify the network system for which the address was required and therefore to provide the required address. The address resolution procedure is completed when the client receives a response from the server containing the required address.



```
rohitdandamudi — -bash — 80x24
Rohits-MacBook-Pro:~ rohitdandamudi$ arp
usage: arp [-n] [-i interface] hostname
       arp [-n] [-i interface] [-l] -a
       arp -d hostname [pub] [ifscope interface]
       arp -d [-i interface] -a
       arp -s hostname ether_addr [temp] [reject] [blackhole] [pub [only]] [ifscope interface]
       arp -S hostname ether_addr [temp] [reject] [blackhole] [pub [only]] [ifscope interface]
       arp -f filename
Rohits-MacBook-Pro:~ rohitdandamudi$ arp google.com
google.com (172.217.163.78) -- no entry
Rohits-MacBook-Pro:~ rohitdandamudi$ arp ww.google.com
ww.google.com (172.217.166.110) -- no entry
Rohits-MacBook-Pro:~ rohitdandamudi$ arp www.google.com
www.google.com (216.58.200.132) -- no entry
Rohits-MacBook-Pro:~ rohitdandamudi$ _
```

## 7. dig(domain information groper):

- Dig stands for (Domain Information Groper) is a network administration command-line tool for querying Domain Name System (DNS) name servers. It is useful for verifying and troubleshooting DNS problems and also to perform DNS lookups and displays the answers that are returned from the name server that were queried. dig is part of the BIND domain name server software suite. dig command replaces older tool such as nslookup and the host. dig tool is available in major Linux distributions.

```
rohithdandamudi — -bash — 80x24
Rohits-MacBook-Pro:~ rohithdandamudi$ dig google.com

; <<>> DiG 9.10.6 <<>> google.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 37710
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 512
;; QUESTION SECTION:
;google.com.                IN      A
;; ANSWER SECTION:
google.com.                 167     IN      A      172.217.167.142

;; Query time: 144 msec
;; SERVER: 8.8.8.8#53(8.8.8.8)
;; WHEN: Wed Jul 24 20:03:04 IST 2019
;; MSG SIZE rcvd: 55

Rohits-MacBook-Pro:~ rohithdandamudi$ _
```

## 8. host:

- On unix-like operating systems, the **host** command is a DNSlookup utility, finding the IP address of a domain name. It also performs reverse lookups, finding the domain name associated with an IP address.
- host performs DNS lookups, converting domain names to IP addresses and vice versa. When no arguments or options are given, host prints a short summary of command line arguments and options.

```
rohitdandamudi — -bash — 80x24
Rohits-MacBook-Pro:~ rohitdandamudi$ host -a google.com
Trying "google.com"
Trying "google.com"
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 1130
;; flags: qr rd ra; QUERY: 1, ANSWER: 18, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;google.com.                IN      ANY

;; ANSWER SECTION:
google.com.                 299     IN      A       172.217.167.142
google.com.                 299     IN      AAAA    2404:6800:4007:803::200e
google.com.                 599     IN      MX      20 alt1.aspmx.l.google.com.
google.com.                 3599    IN      TXT     "v=spf1 include:_spf.google.com
~all"
google.com.                 599     IN      MX      10 aspmx.l.google.com.
google.com.                 3599    IN      TXT     "globalsign-smime-dv=CDYX+XFHUw2
wml6/Gb8+59BsH31KzUr6c1l2BPvqKX8="
google.com.                 3599    IN      TXT     "facebook-domain-verification=22
rm551cu4k0ab0bxsw536tlds4h95"
google.com.                 21599   IN      NS      ns3.google.com.
google.com.                 599     IN      MX      40 alt3.aspmx.l.google.com.
google.com.                 21599   IN      CAA     0 issue "pki.goog"
google.com.                 21599   IN      NS      ns4.google.com.
```

## 9. whois:

- whois searches for an object in a WHOIS database. WHOIS is a query and response protocol that is widely used for querying databases that store the registered users of an Internet resource, such as a domain name or IP Address block, but is also used for a wider range of other information.

```
rohithdandamudi — -bash — 80x24
Rohits-MacBook-Pro:~ rohithdandamudi$ whois google.com
% IANA WHOIS server
% for more information on IANA, visit http://www.iana.org
% This query returned 1 object

refer:      whois.verisign-grs.com

domain:     COM

organisation: VeriSign Global Registry Services
address:    12061 Bluemont Way
address:    Reston Virginia 20190
address:    United States

contact:    administrative
name:       Registry Customer Service
organisation: VeriSign Global Registry Services
address:    12061 Bluemont Way
address:    Reston Virginia 20190
address:    United States
phone:      +1 703 925-6999
fax-no:     +1 703 948 3978
e-mail:     info@verisign-grs.com
```

## 10. traceroute:

- A *traceroute* is a function which traces the path from one network to another. It allows us to diagnose the source of many problems.
- To be effective, the traceroute MUST be run during a time when you are experiencing the problem, from a computer that is experiencing the problem. A trace when you are able to connect, or one from another computer, is not helpful. Therefore, you should try to connect to your site again just before you run it. If the problem is no longer occurring, you will have to wait until the next time the problem occurs (if there is a next time) before running your traceroute.

```
rohithdandamudi — traceroute google.com — 80x24
Rohits-MacBook-Pro:~ rohithdandamudi$ traceroute google.com
traceroute to google.com (172.217.26.174), 64 hops max, 52 byte packets
 1  192.168.1.1 (192.168.1.1)  3.920 ms  4.150 ms  3.066 ms
 2  10.144.0.1 (10.144.0.1)  4.651 ms  4.073 ms  4.282 ms
 3  10.229.0.13 (10.229.0.13)  4.963 ms  6.979 ms  *
 4  broadband.actcorp.in (183.82.14.221)  24.279 ms  18.629 ms  9.038 ms
 5  broadband.actcorp.in (183.82.14.134)  28.391 ms  26.865 ms  22.675 ms
 6  72.14.194.18 (72.14.194.18)  22.652 ms  27.862 ms  19.751 ms
 7  * * _
```