

Network lab

> ipconfig (ip address)

```
maryamabdelraheem@mariamMacBook-Pro ~ % ipconfig getifaddr en0
192.168.1.11
maryamabdelraheem@mariamMacBook-Pro ~ %
```

> ipconfig (Mac) == ipconfig/all & ipconfig(windows)

```
maryamabdelraheem@mariamMacBook-Pro ~ % ipconfig
usage: ipconfig <command> <args>
where <command> is one of waitall, getifaddr, ifconfig, getoption, getiflist, getsummary, getpacket, getv6packet, getr
a, getdhcpduid, getdhcpaid, set, setverbose
```

>2. Configure ip adress manually

1.open system settings > choose network> choose network > wifi

Configure IPv4

IP address

Subnet mask

Router 192.168.1.1

DHCP lease Renew DHCP Lease

DHCP client ID (if required) DHCP client ID

Configure IPv6 Automatically

Router Router

IP address

Forget This Network... Cancel OK

Configure IPv4 Manually

IP address 192.168.1.50

Subnet mask 255.255.255.0

Router 192.168.1.1

Configure IPv6 Automatically

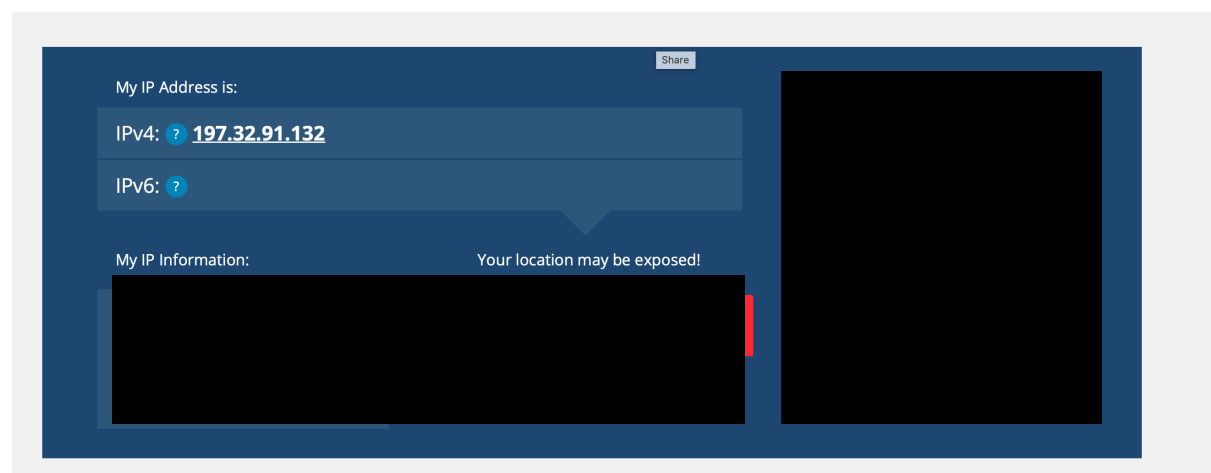
Router Router

IPv6 address fdd4:6ba6:b53b:b200:f5:10e0:b509:ab5

Prefix length 64

Forget This Network... Cancel OK

//whatismyipadress



>>3.ping command

>3.1check connectivity (ping 192.168.1.1)

```
[maryamabdelraheem@mariaMacBook-Pro ~ % ping 192.168.1.1
PING 192.168.1.1 (192.168.1.1): 56 data bytes
64 bytes from 192.168.1.1: icmp_seq=0 ttl=64 time=3.766 ms
64 bytes from 192.168.1.1: icmp_seq=1 ttl=64 time=3.147 ms
64 bytes from 192.168.1.1: icmp_seq=2 ttl=64 time=3.707 ms
64 bytes from 192.168.1.1: icmp_seq=3 ttl=64 time=3.555 ms
64 bytes from 192.168.1.1: icmp_seq=4 ttl=64 time=3.619 ms
64 bytes from 192.168.1.1: icmp_seq=5 ttl=64 time=4.198 ms
64 bytes from 192.168.1.1: icmp_seq=6 ttl=64 time=3.845 ms
64 bytes from 192.168.1.1: icmp_seq=7 ttl=64 time=4.116 ms
64 bytes from 192.168.1.1: icmp_seq=8 ttl=64 time=3.759 ms
64 bytes from 192.168.1.1: icmp_seq=9 ttl=64 time=3.692 ms
64 bytes from 192.168.1.1: icmp_seq=10 ttl=64 time=2.491 ms
64 bytes from 192.168.1.1: icmp_seq=11 ttl=64 time=5.601 ms
64 bytes from 192.168.1.1: icmp_seq=12 ttl=64 time=6.794 ms
64 bytes from 192.168.1.1: icmp_seq=13 ttl=64 time=3.656 ms
64 bytes from 192.168.1.1: icmp_seq=14 ttl=64 time=3.659 ms
64 bytes from 192.168.1.1: icmp_seq=15 ttl=64 time=3.368 ms
64 bytes from 192.168.1.1: icmp_seq=16 ttl=64 time=3.823 ms
64 bytes from 192.168.1.1: icmp_seq=17 ttl=64 time=4.365 ms
64 bytes from 192.168.1.1: icmp_seq=18 ttl=64 time=3.622 ms
█
```

>3.2 check availability of website

```
[maryamabdelraheem@mariaMacBook-Pro ~ % ping google.com
PING google.com (142.251.37.238): 56 data bytes
64 bytes from 142.251.37.238: icmp_seq=0 ttl=117 time=61.014 ms
64 bytes from 142.251.37.238: icmp_seq=1 ttl=117 time=61.912 ms
64 bytes from 142.251.37.238: icmp_seq=2 ttl=117 time=58.840 ms
64 bytes from 142.251.37.238: icmp_seq=3 ttl=117 time=60.326 ms
64 bytes from 142.251.37.238: icmp_seq=4 ttl=117 time=59.407 ms
64 bytes from 142.251.37.238: icmp_seq=5 ttl=117 time=62.051 ms
64 bytes from 142.251.37.238: icmp_seq=6 ttl=117 time=59.708 ms
64 bytes from 142.251.37.238: icmp_seq=7 ttl=117 time=77.731 ms
64 bytes from 142.251.37.238: icmp_seq=8 ttl=117 time=66.871 ms
64 bytes from 142.251.37.238: icmp_seq=9 ttl=117 time=61.227 ms
64 bytes from 142.251.37.238: icmp_seq=10 ttl=117 time=61.855 ms
64 bytes from 142.251.37.238: icmp_seq=11 ttl=117 time=62.276 ms
64 bytes from 142.251.37.238: icmp_seq=12 ttl=117 time=62.036 ms
^C
--- google.com ping statistics ---
13 packets transmitted, 13 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 58.840/62.712/77.731/4.732 ms
maryamabdelraheem@mariaMacBook-Pro ~ % █
```

>3.3 continuous ping (the default)

```
[maryamabdelraheem@mariaMacBook-Pro ~ % ping 192.168.1.1
PING 192.168.1.1 (192.168.1.1): 56 data bytes
64 bytes from 192.168.1.1: icmp_seq=0 ttl=64 time=3.587 ms
64 bytes from 192.168.1.1: icmp_seq=1 ttl=64 time=3.975 ms
64 bytes from 192.168.1.1: icmp_seq=2 ttl=64 time=3.063 ms
64 bytes from 192.168.1.1: icmp_seq=3 ttl=64 time=2.442 ms
^C
--- 192.168.1.1 ping statistics ---
4 packets transmitted, 4 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 2.442/3.267/3.975/0.576 ms
maryamabdelraheem@mariaMacBook-Pro ~ % █
```

>3.4 control number of pings packets

```
maryamabdelraheem@mariaMacBook-Pro ~ % ping -c 7 192.168.1.1
PING 192.168.1.1 (192.168.1.1): 56 data bytes
64 bytes from 192.168.1.1: icmp_seq=0 ttl=64 time=3.546 ms
64 bytes from 192.168.1.1: icmp_seq=1 ttl=64 time=4.090 ms
64 bytes from 192.168.1.1: icmp_seq=2 ttl=64 time=6.677 ms
64 bytes from 192.168.1.1: icmp_seq=3 ttl=64 time=4.931 ms
64 bytes from 192.168.1.1: icmp_seq=4 ttl=64 time=9.810 ms
64 bytes from 192.168.1.1: icmp_seq=5 ttl=64 time=4.478 ms
64 bytes from 192.168.1.1: icmp_seq=6 ttl=64 time=5.398 ms

--- 192.168.1.1 ping statistics ---
7 packets transmitted, 7 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 3.546/5.561/9.810/1.968 ms
maryamabdelraheem@mariaMacBook-Pro ~ %
```

>3.5 control packet size

```
maryamabdelraheem@mariaMacBook-Pro ~ % ping -s 2000 163.121.25.40
PING 163.121.25.40 (163.121.25.40): 2000 data bytes
Request timeout for icmp_seq 0
Request timeout for icmp_seq 1
Request timeout for icmp_seq 2
Request timeout for icmp_seq 3
Request timeout for icmp_seq 4
Request timeout for icmp_seq 5
Request timeout for icmp_seq 6
Request timeout for icmp_seq 7
^C
--- 163.121.25.40 ping statistics ---
9 packets transmitted, 0 packets received, 100.0% packet loss
maryamabdelraheem@mariaMacBook-Pro ~ %
```

>3.6 control packet size AND number of packets

```
maryamabdelraheem@mariaMacBook-Pro ~ % ping -s 2000 -c 6 163.121.12.40
PING 163.121.12.40 (163.121.12.40): 2000 data bytes
Request timeout for icmp_seq 0
Request timeout for icmp_seq 1
Request timeout for icmp_seq 2
Request timeout for icmp_seq 3
Request timeout for icmp_seq 4

--- 163.121.12.40 ping statistics ---
6 packets transmitted, 0 packets received, 100.0% packet loss
maryamabdelraheem@mariaMacBook-Pro ~ %
```

```
maryamabdelraheem@marianMacBook-Pro ~ % ifconfig en0
en0: flags=8863<UP,BROADCAST,SMART,RUNNING,SIMPLEX,MULTICAST> mtu 1500
options=6460<TSO4,TSO6,CHANNEL_IO,PARTIAL_CSUM,ZEROINVERT_CSUM>
ether ae:b8:e8:49:bc:2a
inet6 fe80::181a:db0d:e2a:d234%en0 prefixlen 64 secured scopeid 0xb
inet6 fdd4:6ba6:b53b:b200:f51:10e0:b509:ab5 prefixlen 64 autoconf secured
inet 192.168.1.21 netmask 0xffffff00 broadcast 192.168.1.255
nd6 options=201<PERFORMNUD,DAD>
media: autoselect
status: active
maryamabdelraheem@marianMacBook-Pro ~ %
```

```
maryamabdelraheem@mariamMacBook-Pro ~ % networksetup -getmacaddress en0
Ethernet Address: 3c:06:30:31:4e:7c (Device: en0)
maryamabdelraheem@mariamMacBook-Pro ~ %
```

```
64 bytes from 192.168.1.1: icmp_seq=9 ttl=64 time=3.796 ms
^C
--- 192.168.1.1 ping statistics ---
10 packets transmitted, 10 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 2.637/4.827/7.367/1.321 ms
maryamabdelraheem@mariaMacBook-Pro ~ % arp -a
? (169.254.169.254) at (incomplete) on en0 [ethernet]
? (192.168.1.1) at d4:6b:a6:b5:3b:b2 on en0 ifscope [ethernet]
? (192.168.1.15) at ea:68:58:17:93:b9 on en0 ifscope [ethernet]
? (192.168.1.17) at 8e:80:8f:49:17:51 on en0 ifscope [ethernet]
? (192.168.1.255) at ff:ff:ff:ff:ff:ff on en0 ifscope [ethernet]
mdns.mcast.net (224.0.0.251) at 1:0:5e:0:0:fb on en0 ifscope permanent [ethernet]
? (239.255.255.250) at 1:0:5e:7f:ff:fa on en0 ifscope permanent [ethernet]
```

>6.1 netstat -n

```

yarn@babelrahenmariaMacBook-Pro ~ % netstat -n
Active Internet connections
Proto Rev=Q Send-Q Local Address Foreign Address (state)
tcp4 0 0 192.168.1.21.49648 13.107.213.43.443 ESTABLISHED
tcp4 0 0 192.168.1.21.49641 34.123.33.186.443 ESTABLISHED
tcp4 0 0 192.168.1.21.49620 34.123.33.186.443 ESTABLISHED
tcp4 0 0 192.168.1.21.49619 34.123.33.186.443 ESTABLISHED
tcp4 0 0 192.168.1.21.49618 34.123.33.186.443 ESTABLISHED
tcp4 0 0 192.168.1.21.49616 34.123.33.186.443 ESTABLISHED
tcp4 0 0 192.168.1.21.49586 135.225.242.134.443 ESTABLISHED
tcp4 0 0 192.168.1.21.49584 82.123.159.178.443 ESTABLISHED
tcp4 0 0 192.168.1.21.49580 74.248.74.126.443 ESTABLISHED
tcp4 0 0 192.168.1.21.49578 52.111.231.53.443 ESTABLISHED
tcp4 0 0 192.168.1.21.49572 52.123.134.244.443 ESTABLISHED
tcp4 0 0 192.168.1.21.49568 52.112.122.48.443 ESTABLISHED
tcp4 0 fe80::6fc1:42d4::1025 fe80::c5ab:f7e0::1026 ESTABLISHED
tcp4 0 fe80::6fc1:42d4::1024 fe80::c5ab:f7e0::1024 ESTABLISHED
tcp4 0 192.168.1.11.49494 34.176.65.57.443 ESTABLISHED
tcp4 0 192.168.1.11.49428 216.24.57.7.443 ESTABLISHED
tcp4 0 192.168.1.11.49427 216.24.57.7.443 ESTABLISHED
tcp4 0 fe80::181a:d0b0::49152 fe80::34d1:2bf6f1:c3921 ESTABLISHED
tcp4 0 192.168.1.21.54161 17.248.289.16.443 TIME_WAIT
tcp4 0 192.168.1.21.54160 17.138.128.4.443 ESTABLISHED
tcp4 0 192.168.1.21.54158 17.248.289.16.443 TIME_WAIT
tcp4 0 192.168.1.21.54157 17.248.289.62.443 TIME_WAIT
tcp4 0 192.168.1.21.54156 17.248.289.62.443 TIME_WAIT
tcp4 0 192.168.1.21.54155 17.248.215.129.443 ESTABLISHED
tcp4 548 0 192.168.1.21.54154 17.248.289.62.443 ESTABLISHED
tcp4 0 192.168.1.21.54121 172.64.155.289.443 TIME_WAIT
tcp4 0 192.168.1.21.54058 184.18.32.47.443 ESTABLISHED
tcp4 0 192.168.1.21.54056 172.64.148.171.443 ESTABLISHED
tcp4 0 192.168.1.21.53883 172.64.155.289.443 ESTABLISHED
tcp4 50 192.168.1.21.53872 184.18.39.21.443 ESTABLISHED
tcp4 0 192.168.1.21.53861 17.180.185.138.5223 ESTABLISHED
udp4 0 *.* *.*
udp4 0 *.* *.*
udp4 0 *.* *.*
udp4 0 *.56393 *.*
udp4 0 192.168.1.21.50013 *.*
udp4 0 192.168.1.21.50036 *.*
udp4 0 192.168.1.21.50041 *.*
udp4 0 192.168.1.21.50048 *.*
udp4 0 *.54344 *.*
udp4 0 *.54364 *.*
udp4 0 224.0.0.1.5358 *.*
udp4 0 *.* *.*
udp4 0 *.50088 *.*
udp4 0 *.50075 *.*
udp4 0 *.50438 *.*
udp4 0 *.3722 *.*
udp4 0 *.* *.*

```

>6.2 netstat -a

```
maryamabdelraheem@mariaMacBook-Pro ~ % netstat -a
Active Internet connections (including servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         (state)
tcp4      0      0 192.168.1.21.49672     52.182.143.215.https   ESTABLISHED
tcp4      0      0 192.168.1.21.49671     52.182.143.215.https   ESTABLISHED
tcp4      0      0 192.168.1.21.49670     52.182.143.215.https   ESTABLISHED
tcp4      0      0 192.168.1.21.49669     150.171.22.17.https    ESTABLISHED
tcp4      0      0 192.168.1.21.49668     13.89.179.13.https     ESTABLISHED
tcp4      0      0 192.168.1.21.49658     52.123.133.231.https   ESTABLISHED
tcp4      0      0 192.168.1.21.49656     20.189.173.17.https    ESTABLISHED
tcp4      0      0 192.168.1.21.49655     52.123.129.14.https    ESTABLISHED
tcp4      0      0 192.168.1.21.49654     52.123.129.14.https    ESTABLISHED
tcp4      0      0 192.168.1.21.49653     150.171.22.17.https    ESTABLISHED
tcp4      0      0 192.168.1.21.49652     20.111.1.3.https       ESTABLISHED
tcp4      0      0 192.168.1.21.49651     52.113.194.132.https   ESTABLISHED
tcp4      0      0 192.168.1.21.49650     52.123.129.14.https    ESTABLISHED
tcp4      0      0 192.168.1.21.49641     186.33.123.34.bc.https ESTABLISHED
tcp4      0      0 192.168.1.21.49620     186.33.123.34.bc.https ESTABLISHED
tcp4      0      0 192.168.1.21.49619     186.33.123.34.bc.https ESTABLISHED
tcp4      0      0 192.168.1.21.49618     186.33.123.34.bc.https ESTABLISHED
tcp4      0      0 192.168.1.21.49616     186.33.123.34.bc.https ESTABLISHED
tcp4      0      0 192.168.1.21.49586     135.225.242.134.https  ESTABLISHED
tcp4      0      0 192.168.1.21.49584     52.123.159.178.https   ESTABLISHED
tcp4      0      0 192.168.1.21.49580     74.248.74.126.https    ESTABLISHED
tcp4      0      0 192.168.1.21.49578     52.111.231.53.https    ESTABLISHED
tcp4      0      0 192.168.1.21.49572     52.123.134.244.https   ESTABLISHED
tcp4      0      0 192.168.1.21.49568     52.112.122.48.https    ESTABLISHED
^C
maryamabdelraheem@mariaMacBook-Pro ~ % █
```

>6.3 filter by ipaddress

netstat -an | grep 192.168.1.1

```
[maryamabdelraheem@mariaMacBook-Pro ~ % netstat -an | grep 192.168.1.1
tcp4      0      0 192.168.1.11.49494     34.170.65.59.443       ESTABLISHED
tcp4      0      0 192.168.1.11.49428     216.24.57.7.443        ESTABLISHED
tcp4      0      0 192.168.1.11.49427     216.24.57.7.443        ESTABLISHED
maryamabdelraheem@mariaMacBook-Pro ~ % █
```

>>7. DNS

>7.1 nslookup 87.248.113.14

```
[maryamabdelraheem@mariaMacBook-Pro ~ % nslookup 87.248.113.14
Server:           192.168.1.1
Address:          192.168.1.1#53
```

Non-authoritative answer:
14.113.248.87.in-addr.arpa name = et23-1.bas1-1-edg.amb.yahoo.com.

Authoritative answers can be found from:

```
maryamabdelraheem@mariaMacBook-Pro ~ % █
```

>7.2 nslookup yahoo.com

```
[maryamabdelraheem@mariamMacBook-Pro ~ % nslookup yahoo.com
```

```
Server:          192.168.1.1  
Address:         192.168.1.1#53
```

```
Non-authoritative answer:
```

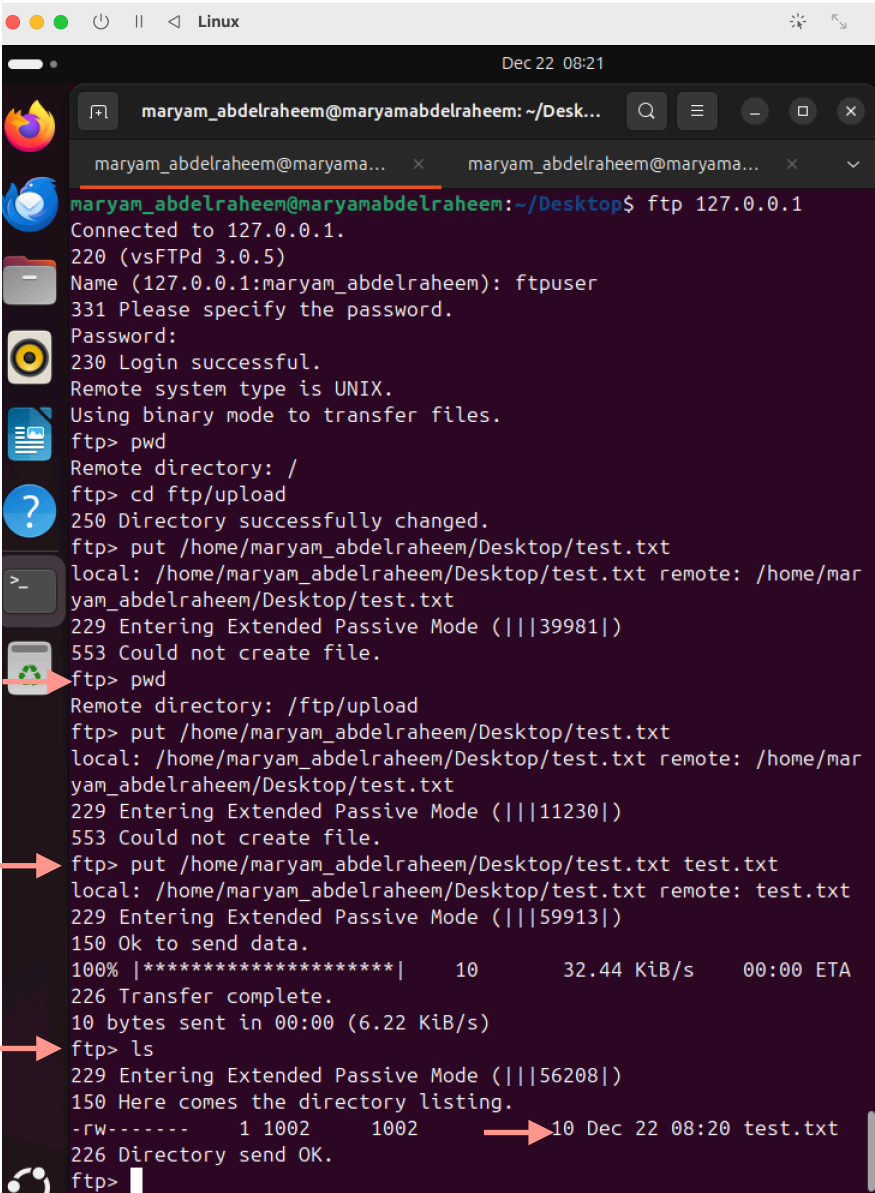
```
Name:   yahoo.com  
Address: 98.137.11.164  
Name:   yahoo.com  
Address: 74.6.143.25  
Name:   yahoo.com  
Address: 74.6.231.20  
Name:   yahoo.com  
Address: 74.6.143.26  
Name:   yahoo.com  
Address: 74.6.231.21  
Name:   yahoo.com  
Address: 98.137.11.163
```

```
maryamabdelraheem@mariamMacBook-Pro ~ % █
```

>>8.port scanning

The built-in FTP service on macOS is deprecated and cannot be enabled on recent versions. Therefore, a Linux virtual machine was used to implement the FTP server with proper authentication, home directory configuration, and authorization.

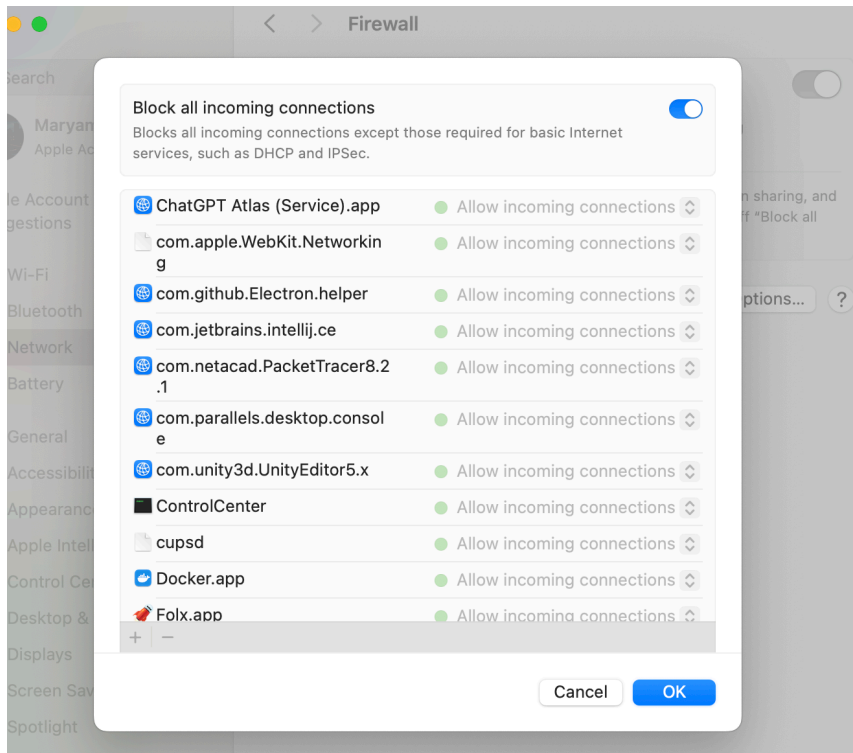
>1.start ftp server



```
Dec 22 08:21
maryam_abdelraheem@maryamabdelraheem: ~/Desk...
maryam_abdelraheem@maryama... x maryam_abdelraheem@maryama... x v
maryam_abdelraheem@maryamabdelraheem:~/Desktop$ ftp 127.0.0.1
Connected to 127.0.0.1.
220 (vsFTPD 3.0.5)
Name (127.0.0.1:maryam_abdelraheem): ftpuser
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> pwd
Remote directory: /
ftp> cd ftp/upload
250 Directory successfully changed.
ftp> put /home/maryam_abdelraheem/Desktop/test.txt
local: /home/maryam_abdelraheem/Desktop/test.txt remote: /home/maryam_abdelraheem/Desktop/test.txt
229 Entering Extended Passive Mode (|||39981|)
553 Could not create file.
ftp> pwd
Remote directory: /ftp/upload
ftp> put /home/maryam_abdelraheem/Desktop/test.txt
local: /home/maryam_abdelraheem/Desktop/test.txt remote: /home/maryam_abdelraheem/Desktop/test.txt
229 Entering Extended Passive Mode (|||11230|)
553 Could not create file.
ftp> put /home/maryam_abdelraheem/Desktop/test.txt test.txt
local: /home/maryam_abdelraheem/Desktop/test.txt remote: test.txt
229 Entering Extended Passive Mode (|||59913|)
150 Ok to send data.
100% |*****| 10 32.44 KiB/s 00:00 ETA
226 Transfer complete.
10 bytes sent in 00:00 (6.22 KiB/s)
ftp> ls
229 Entering Extended Passive Mode (|||56208|)
150 Here comes the directory listing.
-rw----- 1 1002 1002 10 Dec 22 08:20 test.txt
226 Directory send OK.
ftp>
```


>>12. Advanced firewall options

>> 12.1 block all incoming connections



>after blocking the icmp:

```
[maryamabdelraheem@mariamMacBook-Pro ~ % ping 127.0.0.1
PING 127.0.0.1 (127.0.0.1): 56 data bytes
Request timeout for icmp_seq 0
Request timeout for icmp_seq 1
Request timeout for icmp_seq 2
Request timeout for icmp_seq 3
Request timeout for icmp_seq 4
Request timeout for icmp_seq 5
Request timeout for icmp_seq 6
```


>>13. Check malicious website and links

>>12-check

The screenshot shows the VirusShare interface for the URL `http://google.com/`. The top section displays a 'Community Score' of 2717 and a warning: '1/98 security vendor flagged this URL as malicious'. Below this, the 'DETECTION' tab is active, showing a table of security vendors' analysis. The table lists 19 vendors, with 18 reporting 'Clean' and 1 reporting 'Malware' (Cyble). The 'COMMUNITY' tab shows 1.3K members.

Security vendors' analysis	Do you want to automate checks?
Cyble	Malware
Acronis	Clean
AILabs (MONITORAPP)	Clean
alphaMountain.ai	Clean
Artists Against 419	Clean
Bfore.AI PreCrime	Clean
BlockList	Clean
Certego	Clean
Chong Lua Dao	Clean
CMC Threat Intelligence	Clean
Abusix	Clean
ADMINUSLabs	Clean
AlienVault	Clean
Antiy-AVL	Clean
benkow.cc	Clean
BitDefender	Clean
Blueliv	Clean
ChainPatrol	Clean
CINS Army	Clean
CRDF	Clean

malicious software

>check on parallel app

The screenshot shows the VirusShare interface for a file with SHA256 hash `58421e74a052b11cd0a4ecb6e98a57c0ff5fed0a9f9e8b7f11b02c9d46077b7`. The top section displays a 'Community Score' of 0 and a warning: 'No security vendors flagged this file as malicious'. Below this, the 'DETECTION' tab is active, showing a table of security vendors' analysis. The table lists 20 vendors, with 19 reporting 'Undetected' and 1 reporting 'Unable to process file type' (Alibaba). The 'COMMUNITY' tab shows 0 members.

Security vendors' analysis	Do you want to automate checks?
ESET-NOD32	Undetected
GData	Undetected
Gridinsoft (no cloud)	Undetected
Ikarus	Undetected
K7AntiVirus	Undetected
Kaspersky	Undetected
Lionic	Undetected
McAfee Scanner	Undetected
Fortinet	Undetected
Google	Undetected
Huorong	Undetected
Jiangmin	Undetected
K7GW	Undetected
Kingsoft	Undetected
Malwarebytes	Undetected
Microsoft	Undetected
Zillya	Undetected
ZoneAlarm by Check Point	Undetected
Zoner	Undetected
MaxSecure	Timeout
Alibaba	Unable to process file type
Arctic Wolf	Unable to process file type
Avast-Mobile	Unable to process file type
BitDefenderFalx	Unable to process file type
DeepInstinct	Unable to process file type
Elastic	Unable to process file type
Palo Alto Networks	Unable to process file type
SecureAge	Unable to process file type
SentinelOne (Static ML)	Unable to process file type
Symantec Mobile Insight	Unable to process file type
TEHTRIS	Unable to process file type
Trapmine	Unable to process file type
Trustlook	Unable to process file type
Webroot	Unable to process file type