

دستور کار آزمایش شماره 1

عرفان رفیعی اسکویی - 98243027

گام اول)

ابتدا قدم به قدم با راه های گفته شده جلو میرویم :


آدرس ها

Network Connection Details:

Property	Value
Connection-specific DNS ...	192.168.1.1
Description	MediaTek Wi-Fi 6 MT7921 Wireless LAN C
Physical Address	90-E8-68-41-4F-6F
DHCP Enabled	Yes
IPv4 Address	192.168.1.37
IPv4 Subnet Mask	255.255.255.0
Lease Obtained	Friday, February 17, 2023 12:32:09 PM
Lease Expires	Tuesday, February 21, 2023 2:50:50 PM
IPv4 Default Gateway	192.168.1.1
IPv4 DHCP Server	192.168.1.1
IPv4 DNS Server	192.168.1.1
IPv4 WINS Server	
NetBIOS over Tcpip Enab...	Yes
Link-local IPv6 Address	fe80::6274:866d:ba28:564d%23
IPv6 Default Gateway	
IPv6 DNS Server	fe80::1%23

General

Connection

IPv4 Connectivity:	Internet
IPv6 Connectivity:	No network access
Media State:	Enabled
SSID:	Erfan
Duration:	1 day 04:13:18
Speed:	144.4 Mbps
Signal Quality:	

[Details...](#) [Wireless Properties](#)

Activity

	Sent	Received
Bytes:	150,799,088	2,340,433,213

[Properties](#) [Disable](#) [Diagnose](#)

همانطور که مشاهده میشود عمده آدرس ها در کلاس C هستند، و فقط IPV4 Subnet Mask در کلاس خاص E قرار دارد.

گام دوم)

ابتدا یک Folder میسازیم و سپس در قسمت properties آن را برای همه share میکنیم :

Choose people to share with

Type a name and then click Add, or click the arrow to find someone.

→

Name	Permission Level
Erfan Rafiee (efnoskuee@gmail.com)	Owner

[I'm having trouble sharing](#)

Shared Folder Properties

General Sharing Security Previous Versions Customize

Network File and Folder Sharing

Shared Folder
Not Shared

Network Path:
Not Shared

→

Advanced Sharing

Set custom permissions, create multiple shares, and set other advanced sharing options.

Password Protection

People must have a user account and password for this computer to access shared folders.

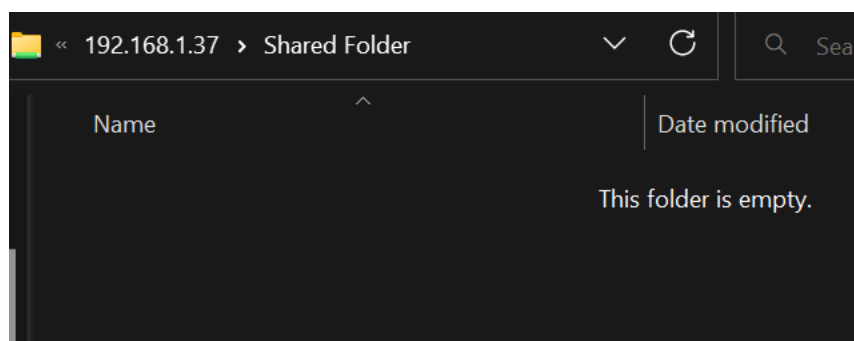
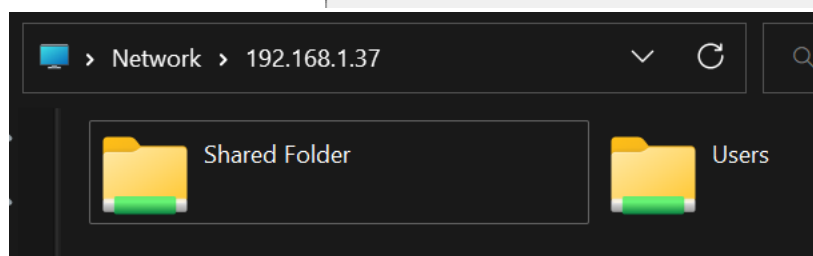
To change this setting, use the [Network and Sharing Center](#).

حال در run آپی مورد نظر که 192.168.1.37 است را میزنیم تا به shared folder ها دسترسی پیدا کنیم :

Run

Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.

Open:



گام سوم)

آدرس فیزیکی :

```
Description . . . . . : Mediatek Wi-Fi 6 E
Physical Address . . . . . : 90-E8-68-41-4F-6F
```

آدرس نام سرور :

```
DNS Servers . . . . . : fe80::1%23
                      192.168.1.1
```

عملکرد دستور ipconfig/all :

در سیستم‌های مبتنی بر ویندوز برای نمایش پیکربندی شبکه TCP/IP فعلی، از جمله آدرس IP، default gateway، subnet mask، آدرس‌های سرور DNS و موارد دیگر استفاده می‌شود. علاوه بر نمایش اطلاعات پیکربندی، این ابزار همچنین می‌تواند برای تنظیم مجدد محتویات حافظه نهان DNS resolver و برای تنظیمات DHCP برای رایانه محلی استفاده شود.

- آدرس سیستم به صورت اتوماتیک تنظیم شده و برای تبدیل آن به صورت دستی مراحل زیر را طی می‌کنیم : (به علت ریسکی بودن این کار فقط مراحل کار آورده شده) (ارجاع شود به بخش 9)

1- Check in which interface autoconfiguration is on.

2- Check for index number of the interface with the command;

`netsh interface ipv4 show inter`

```
C:\Windows\system32>netsh interface ipv4 show inter
Idx  Met      MTU      State      Name
---  -
1     75      4294967295 connected Loopback Pseudo-Interface 1
2     25      1500     connected Ethernet
```

Our index is '2' in this example.

3- Run the command below with changing the '2' with your index number;

`netsh interface ipv4 set interface 2 dadtransmits=0 store=persistent`

```
C:\Windows\system32>netsh interface ipv4 set interface 2 dadtransmits=0 store=persistent
OK.
```

4- Disable DHCP Client service

5- Reboot

دستور ipconfig/release :

Windows IP Configuration

```
No operation can be performed on cfw-tap while it has its media disconnected.  
No operation can be performed on Ethernet while it has its media disconnected.  
No operation can be performed on Ethernet 4 while it has its media disconnected.  
No operation can be performed on Local Area Connection while it has its media disconnected.  
No operation can be performed on Local Area Connection 2 while it has its media disconnected.  
No operation can be performed on Local Area Connection* 1 while it has its media disconnected.  
No operation can be performed on Local Area Connection* 2 while it has its media disconnected.  
No operation can be performed on Ethernet 3 while it has its media disconnected.
```

"IPConfig/release" یک ابزار خط فرمان است که برای انتشار آدرس IP فعلی اختصاص داده

شده توسط یک سرور DHCP استفاده می شود. پیکربندی IP موجود، از جمله تنظیمات دروازه و

DNS را از رایانه حذف می کند، بنابراین آدرس IP آن را برای استفاده توسط دیگران «آزاد» می کند.

دستور ipconfig/renew :

```
C:\Users\efnos>ipconfig/renew
```

Windows IP Configuration

```
No operation can be performed on cfw-tap while it has its media disconnected.  
No operation can be performed on Ethernet while it has its media disconnected.  
No operation can be performed on Local Area Connection 3 while it has its media disconnected.  
No operation can be performed on Ethernet 4 while it has its media disconnected.  
No operation can be performed on Local Area Connection while it has its media disconnected.  
No operation can be performed on Local Area Connection 2 while it has its media disconnected.  
No operation can be performed on Local Area Connection* 1 while it has its media disconnected.  
No operation can be performed on Local Area Connection* 2 while it has its media disconnected.  
No operation can be performed on Ethernet 3 while it has its media disconnected.
```

IPConfig/Renew دستوری در سیستم های ویندوز است که به کاربر اجازه می دهد به صورت دستی

یک آدرس IP (پروتکل اینترنت) را برای دسترسی به اینترنت تمدید کند و کارت رابط شبکه (NIC)

کامپیوتر را مجبور می کند تا یک آدرس IP جدید از پروتکل پیکربندی میزبان پویا (DHCP) به دست آورد.

دستور getmac آدرس فیزیکی سیستم را به ما برمیگرداند :

Physical Address	Transport Name
=====	=====
44-45-53-54-4F-53	Media disconnected
00-FF-42-5E-58-0A	Media disconnected
90-E8-68-41-4F-6F	\Device\Tcpip_{BEC14C90-DE6F-4173-A3A1-CE983F165A66}
04-42-1A-D0-39-38	Media disconnected
00-FF-43-96-AF-A8	Media disconnected
00-FF-8E-D0-FD-58	Media disconnected
N/A	Media disconnected
00-50-56-C0-00-01	\Device\Tcpip_{11490524-E675-4BAF-B6C1-CBE8A3428995}
00-50-56-C0-00-08	\Device\Tcpip_{310E0C82-F5F9-499E-9084-D12E3F1F2489}
00-FF-C5-7A-71-F8	Media disconnected

گام چهارم)

```
C:\Users\efnos>ping 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data:
Reply from 192.168.1.1: bytes=32 time=1ms TTL=64
Reply from 192.168.1.1: bytes=32 time=1ms TTL=64
Reply from 192.168.1.1: bytes=32 time=1ms TTL=64
Reply from 192.168.1.1: bytes=32 time=1ms TTL=64

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 1ms, Average = 1ms

C:\Users\efnos>ping 192.168.1.37

Pinging 192.168.1.37 with 32 bytes of data:
Reply from 192.168.1.37: bytes=32 time<1ms TTL=128
Reply from 192.168.1.37: bytes=32 time<1ms TTL=128
Reply from 192.168.1.37: bytes=32 time<1ms TTL=128
Reply from 192.168.1.37: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.1.37:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

حال ارتباط با google را چک میکنیم :

```
C:\Users\efnos>ping www.google.com

Pinging www.google.com [216.239.38.120] with 32 bytes of data:
Reply from 216.239.38.120: bytes=32 time=146ms TTL=107
Reply from 216.239.38.120: bytes=32 time=147ms TTL=107
Reply from 216.239.38.120: bytes=32 time=146ms TTL=107
Reply from 216.239.38.120: bytes=32 time=147ms TTL=107

Ping statistics for 216.239.38.120:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 146ms, Maximum = 147ms, Average = 146ms
```

پیغام خاصی مشاهده نشد و مانند ping قبلی بود.

گام پنجم)

```
C:\Users\efnos>tracert www.google.com

Tracing route to www.google.com [216.239.38.120]
over a maximum of 30 hops:

  0  <1 ms    <1 ms    <1 ms    192.168.1.1
  1  28 ms     25 ms     26 ms     2.177.128.1
  2  *          28 ms     26 ms     93.118.125.41
  3  *          *          *          Request timed out.
  4  *          28 ms     26 ms     5.239.247.5
  5  26 ms     26 ms     *          10.21.252.18
  6  26 ms     25 ms     25 ms     10.202.7.102
  7  28 ms     27 ms     26 ms     10.21.21.10
  8  58 ms     59 ms     60 ms     134.0.220.186
  9  61 ms     62 ms     60 ms     213.202.5.239
 10  59 ms     59 ms     59 ms     216.239.48.87
 11  63 ms     64 ms     69 ms     108.170.227.189
 12  134 ms    131 ms    135 ms    any-in-2678.1e100.net [216.239.38.120]

Trace complete.
```

علت وقوع time out میتواند به این دلیل باشد که ICMP (پروتکل مورد استفاده توسط traceroute) دارای کمترین اولویت است، و هنگامی که ترافیک با اولویت بالاتر در حال انجام

است، روتر ممکن است به گونه ای پیکربندی شود که بسته های ICMP را به سادگی رها کند. همچنین این احتمال وجود دارد که ISP تمام بسته های ICMP را به عنوان یک موضوع امنیتی حذف کند زیرا بسیاری از حملات DOS (Denial of Service) بر اساس بررسی انجام شده با بسته های ICMP هستند.

گام ششم)

```
C:\Users\efnos>nslookup
Default Server:  UnKnown
Address:  fe80::1
```

```
C:\Users\efnos>nslookup www.google.com
Server:  UnKnown
Address:  fe80::1

Non-authoritative answer:
Name:    www.google.com
Addresses:  2a00:1450:400f:804::2004
            142.250.186.36
```

```
C:\Users\efnos>nslookup www.yahoo.com
Server:  UnKnown
Address:  fe80::1

Non-authoritative answer:
Name:    new-fp-shed.wg1.b.yahoo.com
Addresses:  2a00:1288:110:c305::1:8001
            2a00:1288:110:c305::1:8000
            87.248.100.216
            87.248.100.215
Aliases:  www.yahoo.com
```

گام هفتم)

جدول اطلاعات :

Interface: 192.168.43.1 --- 0x6			
Internet Address	Physical Address	Type	
192.168.43.254	00-50-56-fe-bd-13	dynamic	
192.168.43.255	ff-ff-ff-ff-ff-ff	static	
224.0.0.22	01-00-5e-00-00-16	static	
224.0.0.251	01-00-5e-00-00-fb	static	
224.0.0.252	01-00-5e-00-00-fc	static	
239.255.255.250	01-00-5e-7f-ff-fa	static	
255.255.255.255	ff-ff-ff-ff-ff-ff	static	
Interface: 192.168.52.1 --- 0xa			
Internet Address	Physical Address	Type	
192.168.52.254	00-50-56-fc-0c-96	dynamic	
192.168.52.255	ff-ff-ff-ff-ff-ff	static	
224.0.0.22	01-00-5e-00-00-16	static	
224.0.0.251	01-00-5e-00-00-fb	static	
224.0.0.252	01-00-5e-00-00-fc	static	
239.255.255.250	01-00-5e-7f-ff-fa	static	
255.255.255.255	ff-ff-ff-ff-ff-ff	static	
Interface: 192.168.1.37 --- 0x17			
Internet Address	Physical Address	Type	
192.168.1.1	e4-18-6b-db-51-88	dynamic	
192.168.1.33	cc-6e-a4-2b-f7-56	dynamic	
192.168.1.36	98-22-ef-27-96-db	dynamic	
192.168.1.255	ff-ff-ff-ff-ff-ff	static	
224.0.0.22	01-00-5e-00-00-16	static	
224.0.0.251	01-00-5e-00-00-fb	static	
224.0.0.252	01-00-5e-00-00-fc	static	
239.255.255.250	01-00-5e-7f-ff-fa	static	
255.255.255.255	ff-ff-ff-ff-ff-ff	static	
Interface: 10.9.27.219 --- 0x3f			
Internet Address	Physical Address	Type	
8.241.9.126		dynamic	
8.241.9.254		dynamic	
8.241.121.254		dynamic	
8.241.122.126		dynamic	
8.241.123.126		dynamic	
8.241.123.254		dynamic	
8.248.113.254		dynamic	
8.248.147.254		dynamic	
8.250.161.254		dynamic	
8.250.197.254		dynamic	
8.250.203.254		dynamic	
8.252.42.254		dynamic	
8.252.73.126		dynamic	
8.252.189.126		dynamic	
8.253.246.254		dynamic	
10.8.0.1		dynamic	
20.253.213.245		dynamic	
184.24.14.183		dynamic	
224.0.0.22		static	
224.0.0.251		static	

Displays and modifies the IP-to-Physical address translation tables used by address resolution protocol (ARP).

ARP -s inet_addr eth_addr [if_addr]

ARP -d inet_addr [if_addr]

ARP -a [inet_addr] [-N if_addr] [-v]

-a Displays current ARP entries by interrogating the current protocol data. If inet_addr is specified, the IP and Physical addresses for only the specified computer are displayed. If more than one network interface uses ARP, entries for each ARP table are displayed.

-g Same as -a.

-v Displays current ARP entries in verbose mode. All invalid entries and entries on the loop-back interface will be shown.

inet_addr Specifies an internet address.

-N if_addr Displays the ARP entries for the network interface specified by if_addr.

-d Deletes the host specified by inet_addr. inet_addr may be wildcarded with * to delete all hosts.

-s Adds the host and associates the Internet address inet_addr with the Physical address eth_addr. The Physical address is given as 6 hexadecimal bytes separated by hyphens. The entry is permanent.

eth_addr Specifies a physical address.

if_addr If present, this specifies the Internet address of the interface whose address translation table should be modified. If not present, the first applicable interface will be used.

Example:

> arp -s 157.55.85.212 00-aa-00-62-c6-09 Adds a static entry.

> arp -a Displays the arp table.

اضافه کردن آدرس سیستم :

تغییرات ایجاد شده

Internet Address	Physical Address	Type
192.168.1.1	e4-18-6b-db-51-88	dynamic
192.168.1.33	cc-6e-a4-2b-f7-56	dynamic
192.168.1.36	98-22-ef-27-96-db	dynamic
192.168.1.37	90-e8-68-41-4f-6f	static
192.168.1.255	ff-ff-ff-ff-ff-ff	static
224.0.0.22	01-00-5e-00-00-16	static
224.0.0.251	01-00-5e-00-00-fb	static
224.0.0.252	01-00-5e-00-00-fc	static
239.255.255.250	01-00-5e-7f-ff-fa	static
255.255.255.255	ff-ff-ff-ff-ff-ff	static

حذف کردن آدرس سیستم :

```
C:\Windows\System32>arp -d 192.168.1.37
```

تغییرات :

```
Interface: 192.168.1.37 --- 0x17
Internet Address      Physical Address      Type
192.168.1.1           e4-18-6b-db-51-88    dynamic
192.168.1.33           cc-6e-a4-2b-f7-56    dynamic
192.168.1.36           98-22-ef-27-96-db    dynamic
192.168.1.255          ff-ff-ff-ff-ff-ff    static
224.0.0.22             01-00-5e-00-00-16    static
224.0.0.251            01-00-5e-00-00-fb    static
224.0.0.252            01-00-5e-00-00-fc    static
239.255.255.250        01-00-5e-7f-ff-fa    static
255.255.255.255        ff-ff-ff-ff-ff-ff    static
```

گام هشتم)

دستور netstat -n شماره های port و آدرس هارا به صورت numerical نشان میدهد :

```
C:\Windows\System32>netstat -n

Active Connections

Proto Local Address          Foreign Address         State
TCP    127.0.0.1:1042          127.0.0.1:54415        ESTABLISHED
TCP    127.0.0.1:1042          127.0.0.1:54476        ESTABLISHED
TCP    127.0.0.1:1042          127.0.0.1:60975        ESTABLISHED
TCP    127.0.0.1:9012          127.0.0.1:54459        ESTABLISHED
TCP    127.0.0.1:9013          127.0.0.1:60976        ESTABLISHED
TCP    127.0.0.1:17532         127.0.0.1:54401        ESTABLISHED
TCP    127.0.0.1:54315         127.0.0.1:65001        ESTABLISHED
TCP    127.0.0.1:54401         127.0.0.1:17532        ESTABLISHED
TCP    127.0.0.1:54414         127.0.0.1:60972        ESTABLISHED
TCP    127.0.0.1:54415         127.0.0.1:1042         ESTABLISHED
TCP    127.0.0.1:54459         127.0.0.1:9012         ESTABLISHED
TCP    127.0.0.1:54476         127.0.0.1:1042         ESTABLISHED
TCP    127.0.0.1:60972         127.0.0.1:54414        ESTABLISHED
TCP    127.0.0.1:60975         127.0.0.1:1042         ESTABLISHED
TCP    127.0.0.1:60976         127.0.0.1:9013         ESTABLISHED
TCP    127.0.0.1:65001         127.0.0.1:54315        ESTABLISHED
TCP    192.168.1.37:52264      64.233.184.188:5228    ESTABLISHED
TCP    192.168.1.37:57617      104.77.36.175:80        ESTABLISHED
TCP    192.168.1.37:57618      104.208.16.90:443       ESTABLISHED
TCP    192.168.1.37:61809      142.250.185.194:443    TIME_WAIT
TCP    192.168.1.37:61810      142.250.185.98:443     TIME_WAIT
TCP    192.168.1.37:61875      2.23.209.182:443       CLOSE_WAIT
TCP    192.168.1.37:61882      2.16.241.92:443        ESTABLISHED
TCP    192.168.1.37:61883      2.16.241.92:443        CLOSE_WAIT
TCP    192.168.1.37:61884      2.16.241.92:443        CLOSE_WAIT
TCP    192.168.1.37:61885      2.16.241.92:443        CLOSE_WAIT
TCP    192.168.1.37:61886      2.16.241.92:443        CLOSE_WAIT
TCP    192.168.1.37:61887      2.16.241.92:443        CLOSE_WAIT
TCP    192.168.1.37:63157      20.198.119.84:443      ESTABLISHED
TCP    192.168.1.37:63913      87.250.250.90:443      ESTABLISHED
```

دستور netstat -a -n تمامی connection ها و listening port ها را به صورت

numerical نشان میدهد :

[illegible]

پروتکل های مورد پشتیبانی توسط netstat -p :

may be any of: TCP, UDP, TCPv6, or UDPv6.

گام نهم)

تغییر IP سیستم :

```
C:\Users\efnos>netsh interface ipv4 show interfaces
```

Idx	Met	MTU	State	Name
1	75	4294967295	connected	Loopback Pseudo-Interface 1
12	25	1500	disconnected	Local Area Connection
23	0	1500	connected	Wi-Fi
22	5	1500	disconnected	Ethernet
20	25	1500	disconnected	Local Area Connection 2
8	25	1500	disconnected	Local Area Connection* 1
7	5	1500	disconnected	Local Area Connection 3
15	25	1500	disconnected	Local Area Connection* 2
14	35	1400	disconnected	Ethernet 3
13	6	1500	disconnected	Ethernet 4
58	1	1500	disconnected	cfw-tap

```
C:\Users\efnos>netsh interface ipv4 show addresses "Wi-Fi"
```

Configuration for interface "Wi-Fi"

DHCP enabled:	Yes
IP Address:	192.168.1.37
Subnet Prefix:	192.168.1.0/24 (mask 255.255.255.0)
Default Gateway:	192.168.1.1
Gateway Metric:	0
InterfaceMetric:	0

حال دستور تغییر را زده و دوباره چک میکنیم :

```
Microsoft Windows [Version 10.0.22621.1265]
```

```
(c) Microsoft Corporation. All rights reserved.
```

```
C:\Windows\System32>netsh interface ipv4 set address name="Wi-Fi" source=static address=192.168.58.3 mask=255.255.255.0 gateway=192.168.1.1
```

```
C:\Windows\System32>netsh interface ipv4 show addresses "Wi-Fi"
```

Configuration for interface "Wi-Fi"

DHCP enabled:	No
IP Address:	192.168.58.3
Subnet Prefix:	192.168.58.0/24 (mask 255.255.255.0)
Default Gateway:	192.168.1.1
Gateway Metric:	1
InterfaceMetric:	0

همانطور که در عکس ها مشاهده شد تغییرات را ایجاد کردیم.

درخواست IP جدید :

میبینیم که DHCP غیر فعال است :

```
C:\Windows\System32>netsh interface ipv4 show addresses "Wi-Fi"

Configuration for interface "Wi-Fi"
    DHCP enabled:                No
    IP Address:                  192.168.58.3
    Subnet Prefix:               192.168.58.0/24 (mask 255.255.255.0)
    Default Gateway:            192.168.1.1
    Gateway Metric:              1
    InterfaceMetric:            0
```

برای گرفتن IP داینامیک از dhcp دستور زیر را ران میکنیم :

```
C:\Windows\System32>netsh interface ipv4 set address name="Wi-Fi" source=dhcp
```

حال دوباره چک میکنیم :

```
Configuration for interface "Wi-Fi"
    DHCP enabled:                Yes
    IP Address:                  192.168.1.38
    Subnet Prefix:               192.168.1.0/24 (mask 255.255.255.0)
    Default Gateway:            192.168.1.1
    Gateway Metric:              0
    InterfaceMetric:            0
```

میبینیم که ip جدید را گرفتیم.

تغییر DNS server به صورت دستی :



Network & internet



Wi-Fi

Connect, manage known networks, metered network

On



Erfan properties

Connected, secured



DNS server assignment:

Automatic (DHCP)

Edit

Edit network DNS settings

Manual



IPv4



On

Preferred DNS

18.72.0.3



DNS over HTTPS

Off



Alternate DNS

DNS over HTTPS

Off



IPv6



Off