

# 重庆交通大学信息科学与工程学院

## 实 验 报 告

班 级： 曙光 1901 班

姓名 学号： 樊宇杰 631907060603

实验项目名称： 计算机网络 XXXXX

实验项目性质： 验证性

实验所属课程： 计算机网络

实验室(中心)： 计算中心三机房

指导教师： 王勇

实验完成时间： 2021 年 9 月 20 日

## 一、实验概述：

### 【实验目的】

1. 了解计算机网络常用命令
2. 掌握
3. 掌握

### 【实施环境】（使用的材料、设备、软件）

Windows 操作系统环境, cmd,powershell

## 二、实验内容

### 第 1 题 查看自己计算机的网络配置

#### 【实验过程】（步骤、记录、数据、程序等）

Cmd 输入 ipconfig/all

Windows IP 配置

主机名 .....: DESKTOP-LF4P0S5  
主 DNS 后缀 .....:  
节点类型 .....: 混合  
IP 路由已启用 .....: 否  
WINS 代理已启用 .....: 否

以太网适配器 SSTAP 1:

媒体状态 .....: 媒体已断开连接  
连接特定的 DNS 后缀 .....:  
描述.....: TAP-Windows Adapter V9 #2  
物理地址.....: 00-FF-87-93-5D-D2  
DHCP 已启用 .....: 否  
自动配置已启用.....: 是

以太网适配器 cfw-tap:

媒体状态 .....: 媒体已断开连接  
连接特定的 DNS 后缀 .....:  
描述.....: TAP-Windows Adapter V9 #3  
物理地址.....: 00-FF-86-21-A4-64  
DHCP 已启用 .....: 是

自动配置已启用.....: 是

未知适配器 aioCloud:

媒体状态 .....: 媒体已断开连接  
连接特定的 DNS 后缀 .....:  
描述.....: WireGuard Tunnel  
物理地址.....:  
DHCP 已启用 .....: 否  
自动配置已启用.....: 是

以太网适配器 以太网 2:

媒体状态 .....: 媒体已断开连接  
连接特定的 DNS 后缀 .....:  
描述.....: TAP-Windows Adapter V9  
物理地址.....: 00-FF-49-B0-FC-1C  
DHCP 已启用 .....: 是  
自动配置已启用.....: 是

无线局域网适配器 本地连接\* 2:

媒体状态 .....: 媒体已断开连接  
连接特定的 DNS 后缀 .....:  
描述.....: Microsoft Wi-Fi Direct Virtual Adapter #5  
物理地址.....: F4-D1-08-5E-40-8A  
DHCP 已启用 .....: 是  
自动配置已启用.....: 是

无线局域网适配器 本地连接\* 3:

媒体状态 .....: 媒体已断开连接  
连接特定的 DNS 后缀 .....:  
描述.....: Microsoft Wi-Fi Direct Virtual Adapter #6  
物理地址.....: F6-D1-08-5E-40-89  
DHCP 已启用 .....: 否  
自动配置已启用.....: 是

以太网适配器 以太网 5:

媒体状态 .....: 媒体已断开连接  
连接特定的 DNS 后缀 .....:  
描述.....: Netease UU TAP-Win32 Adapter V9.21  
物理地址.....: 00-FF-95-83-4A-4B

```
DHCP 已启用 .....: 否
自动配置已启用.....: 是
```

以太网适配器 以太网 4:

```
媒体状态 .....: 媒体已断开连接
连接特定的 DNS 后缀 .....:
描述.....: Sangfor SSL VPN CS Support System VNIC
物理地址.....: 00-FF-2F-BF-EE-16
DHCP 已启用 .....: 否
自动配置已启用.....: 是
```

以太网适配器 以太网:

```
媒体状态 .....: 媒体已断开连接
连接特定的 DNS 后缀 .....:
描述.....: Realtek PCIe GbE Family Controller
物理地址.....: 80-FA-5B-67-19-F3
DHCP 已启用 .....: 是
自动配置已启用.....: 是
```

以太网适配器 以太网 3:

```

连接特定的 DNS 后缀 .....:
描述.....: ZTE CMCC NDIS Interface
物理地址.....: 00-A0-C6-00-00-16
DHCP 已启用 .....: 是
自动配置已启用.....: 是
本地链接 IPv6 地址.....: fe80::70b4:de9d:5872:2a37%4(首选)
IPv4 地址 .....: 10.63.53.250(首选)
子网掩码 .....: 255.0.0.0
获得租约的时间 .....: 2021 年 9 月 15 日 8:17:15
租约过期的时间 .....: 2021 年 9 月 15 日 10:17:14
默认网关.....: 10.63.53.251
DHCP 服务器 .....: 10.63.53.251
DHCPv6 IAID .....: 973119686
DHCPv6 客户端 DUID .....: 00-01-00-01-24-C1-F8-FE-80-FA-5B-67-19-F3
DNS 服务器 .....: 183.230.126.225
                                183.230.126.224
TCP/IP 上的 NetBIOS .....: 已启用

```

## 无线局域网适配器 WLAN:

媒体状态 .....: 媒体已断开连接



来自 202.202.240.102 的回复: 字节=32 时间=30ms TTL=46

来自 202.202.240.102 的回复: 字节=32 时间=36ms TTL=46

202.202.240.102 的 Ping 统计信息:

数据包: 已发送 = 4, 已接收 = 4, 丢失 = 0 (0% 丢失),  
往返行程的估计时间(以毫秒为单位):

最短 = 30ms, 最长 = 36ms, 平均 = 33ms

(Time To Live), 当报文在网络中转发时, 时间超过这个限制, 最后一个收到报文的路由点就会把它扔掉, 而不继续转发。

#### 第 4 题 使用 ping/? 命令了解该命令的各种选项并实际使用

【实验过程】(步骤、记录、数据、程序等)

#### 第 5 题 大致清楚本机到百度服务器之间的路径

【实验过程】(步骤、记录、数据、程序等)

通过最多 30 个跃点跟踪

到 www.a.shifen.com [183.232.231.172] 的路由:

1	*	*	*	请求超时。
2	36 ms	26 ms	25 ms	10.10.13.5
3	35 ms	50 ms	33 ms	10.10.13.49
4	*	*	*	请求超时。
5	117 ms	26 ms	38 ms	183.230.99.18
6	34 ms	39 ms	47 ms	ptr.cq.chinamobile.com [218.206.9.253]
7	30 ms	27 ms	33 ms	ptr.cq.chinamobile.com [218.206.9.42]
8	37 ms	27 ms	29 ms	221.183.49.41
9	*	*	*	请求超时。
10	*	*	*	请求超时。
11	59 ms	57 ms	58 ms	120.241.49.30
12	*	*	*	请求超时。
13	*	*	*	请求超时。
14	*	*	*	请求超时。
15	*	*	*	请求超时。
16	*	*	*	请求超时。
17	*	*	*	请求超时。
18	*	*	*	请求超时。
19	*	*	*	请求超时。
20	*	*	*	请求超时。

21	*	*	*	请求超时。
22	*	*	*	请求超时。
23	*	*	*	请求超时。
24	*	*	*	请求超时。
25	*	*	*	请求超时。
26	*	*	*	请求超时。
27	*	*	*	请求超时。
28	*	*	*	请求超时。
29	*	*	*	请求超时。
30	*	*	*	请求超时。
1	*	*	*	请求超时。
2	49 ms	81 ms	25 ms	10.10.13.5
3	36 ms	28 ms	26 ms	10.10.13.49
4	*	*	*	请求超时。
5	38 ms	33 ms	46 ms	183.230.99.18
6	21 ms	27 ms	29 ms	ptr.cq.chinamobile.com [218.206.9.253]
7	30 ms	30 ms	33 ms	ptr.cq.chinamobile.com [218.206.9.42]
8	28 ms	28 ms	*	221.183.49.41
9	*	*	*	请求超时。
10	*	*	*	请求超时。
11	53 ms	58 ms	57 ms	120.241.49.194
12	*	*	*	请求超时。
13	68 ms	62 ms	47 ms	ptr.cq.chinamobile.com [183.232.231.174]

一.

二. 第一个就是局域网出口路由器，从局域网出来必然会经过此路由器，后面这几个路由器管理对应一块区域的通信，局域网的路由器以它们为中心相联；

三. \*表示路径上的路由器 没有返回 ICMP TTL 包或者返回对应的包丢失 有可能到对应的路由器超过了 ttl 或者对应服务器不接受 ping 包

## 第 6 题 浏览器访问 <http://ping.pe/qige.io>

【实验过程】（步骤、记录、数据、程序等）

```
Canada, BC, Vancouver    Shaw 0% 68 14.2 15.31 12.07 23.89 2.06 show
USA, CA, Fremont        Hurricane FMT2 1.5% 67 2.15 49.06 2.14 1797.83 266.26 show
USA, CA, Fremont        Linode 0% 68 1.14 1.41 1.1 2.25 0.44 show
USA, CA, San Francisco  Digital Ocean 0% 69 2.14 1.97 1.16 4.18 0.52 show
USA, CA, Los Angeles    QuadraNET 0% 69 2.39 3.98 1.2 16.05 2.88 show
USA, CA, Los Angeles    Vultr 0% 69 1.12 1.16 1.09 2.19 0.13 show
USA, CA, Seattle        Google 0% 68 7.52 7.6 7.49 7.8 0.07 show
USA, CO, Denver         Cogent 0% 68 24.91 24.35 3.03 27.43 2.8 show
```

USA, TX, Dallas	Softlayer	0%	68	3.44	2.75	2.3	4.12	0.55	show
USA, IL, Chicago	Cogent	0%	68	2.44	3.05	1.41	9.86	1.26	show
USA, GA, Atlanta	55 Marietta/RamNode	0%	68	1.12	1.4	1.07	6.39	0.96	show
USA, VA, Vint Hill	OVH	0%	68	2.25	2.35	2.16	5.37	0.49	show
USA, NY, New York	Telehouse/RamNode	0%	68	2.19	2.24	2.11	5.4	0.4	show
Canada, QC, Montreal	OVH	0%	68	8.79	8.79	8.72	9.28	0.08	show
France, Paris	Online.net	0%	66	16.66	16.67	15.86	16.95	0.13	show
Netherlands, Amsterdam	Online.net	0%	68	7.81	7.86	7.68	8.89	0.29	show
Netherlands, Nuland	WeservIT/RamNode	0%	67	10.72	9.94	9.49	10.84	0.46	show
Norway, Sandefjord	Terrahost	0%	66	3.4	3.35	3.25	3.43	0.05	show
Germany, Nuremberg	Hetzner	0%	66	4.61	4.57	4.32	7.68	0.44	show
Italy, Milan	Prometeus	0%	66	1.2	1.38	1.11	6.89	0.9	show
Singapore	Digital Ocean	0%	66	1.09	1.12	1.08	2.17	0.13	show
Japan, Tokyo	Vultr	0%	68	1.16	1.39	1.1	2.34	0.45	show
Australia, Sydney	Vultr	0%	66	2.29	2.25	2.17	2.39	0.05	show
Taiwan, Taichung	Google	0%	64	37.61	36.97	33.95	38.91	1.34	show
China, Shenzhen	Aliyun	0%	62	161.84		159.39	49.55	163.11	14.41 show
China, Beijing	Aliyun	0%	60	259.98		230.33	20.56	491.26	50.76 show
China, Beijing	Tencent	1.6%	61	350.53		160.28	4.35	350.53	33.79 show
China, Quanzhou	China Telecom CN2	0%	18	58.22	58.54	57.86	60.03	0.53	show
China, Jiangsu	China Telecom	0%	62	149.26		143.97	8.4	149.34	22.57 show
China, Jiangsu	China Mobile	8.5%	59	204.67		310.51	7.1	1919.36	374.54 show
China, Jiangsu	China Unicom	0%	61	268.25		259.35	12.75	646.58	64.94 show
China, Hangzhou	Aliyun	0%	61	268.75		221.01	18.54	269.11	61.37 show
China, Qingdao	Aliyun	6.8%	59	266.41		213.57	9.96	269.93	66.06 show
China, Shanghai	Aliyun	0%	61	203.94		232.55	35.76	274.51	46.23 show

## 第7题 ARP

【实验过程】（步骤、记录、数据、程序等）

实作一

运行 `arp -a` 命令查看当前的 `arp` 缓存， 请留意缓存了些什么。

Internet 地址	物理地址	类型
10.0.0.1	00-1b-fc-9a-a4-00	动态
10.13.231.143	00-1b-fc-9a-a4-00	动态
10.102.127.241	00-1b-fc-9a-a4-00	动态
10.255.255.255	ff-ff-ff-ff-ff-ff	静态
169.254.169.254	00-1b-fc-9a-a4-00	动态
224.0.0.22	01-00-5e-00-00-16	静态
224.0.0.251	01-00-5e-00-00-fb	静态
224.0.0.252	01-00-5e-00-00-fc	静态
239.11.20.1	01-00-5e-0b-14-01	静态



239.255.255.250	01-00-5e-7f-ff-fa	静态
255.255.255.255	ff-ff-ff-ff-ff-ff	静态

然后 ping 一下你旁边的计算机 IP（注意，需保证该计算机的 IP 没有出现在 arp 缓存中，或者使用 arp -d \* 先删除全部缓存），再次查看缓存，你会发现一些改变，请作出解释。

ping 183.232.231.172

正在 Ping 183.232.231.172 具有 32 字节的数据:

来自 183.232.231.172 的回复: 字节=32 时间=55ms TTL=52

来自 183.232.231.172 的回复: 字节=32 时间=60ms TTL=52

来自 183.232.231.172 的回复: 字节=32 时间=57ms TTL=52

来自 183.232.231.172 的回复: 字节=32 时间=54ms TTL=52

183.232.231.172 的 Ping 统计信息:

数据包: 已发送 = 4, 已接收 = 4, 丢失 = 0 (0% 丢失),  
往返行程的估计时间(以毫秒为单位):

最短 = 54ms, 最长 = 60ms, 平均 = 56ms

接口: 10.102.127.240 --- 0x4

Internet 地址	物理地址	类型
10.0.0.1	00-1b-fc-9a-a4-00	动态
10.13.231.143	00-1b-fc-9a-a4-00	动态
10.102.127.241	00-1b-fc-9a-a4-00	动态
10.162.160.229	00-1b-fc-9a-a4-00	动态
10.255.255.255	ff-ff-ff-ff-ff-ff	静态
169.254.169.254	00-1b-fc-9a-a4-00	动态
224.0.0.22	01-00-5e-00-00-16	静态
224.0.0.251	01-00-5e-00-00-fb	静态
224.0.0.252	01-00-5e-00-00-fc	静态
239.11.20.1	01-00-5e-0b-14-01	静态
239.255.255.250	01-00-5e-7f-ff-fa	静态
255.255.255.255	ff-ff-ff-ff-ff-ff	静态

实作二

请使用 arp /? 命令了解该命令的各种选项。

-a                    通过询问当前协议数据，显示当前 ARP 项。  
如果指定 inet\_addr，则只显示指定计算机的 IP 地址和物理地址。如果不止一个网络接口使用 ARP，则显示每个 ARP 表的项。

-g 与 -a 相同。

-v 在详细模式下显示当前 ARP 项。所有无效项和环回接口上的项都将显示。

inet\_addr 指定 Internet 地址。

-N if\_addr 显示 if\_addr 指定的网络接口的 ARP 项。

-d 删除 inet\_addr 指定的主机。inet\_addr 可以是通配符 \*，以删除所有主机。

-s 添加主机并且将 Internet 地址 inet\_addr 与物理地址 eth\_addr 相关联。物理地址是用连字符分隔的 6 个十六进制字节。该项是永久的。

eth\_addr 指定物理地址。

if\_addr 如果存在，此项指定地址转换表应修改的接口的 Internet 地址。如果不存在，则使用第一个适用的接口。

示例:

```
> arp -s 157.55.85.212 00-aa-00-62-c6-09.... 添加静态项。
> arp -a .... 显示 ARP 表。
```

### 实作三

一般而言，arp 缓存里常常会有网关的缓存，并且是动态类型的。

假设当前网关的 IP 地址是 192.168.0.1，MAC 地址是 5c-d9-98-f1-89-64，请使用 arp -s 192.168.0.1 5c-d9-98-f1-89-64 命令设置其为静态类型的。

接口: 10.80.146.218 --- 0x4

Internet 地址	物理地址	类型
10.0.0.1	00-1b-fc-9a-a4-00	动态
10.13.231.143	00-1b-fc-9a-a4-00	动态
10.80.146.219	00-1b-fc-9a-a4-00	动态
10.102.149.133	00-1b-fc-9a-a4-00	动态
10.123.246.87	00-1b-fc-9a-a4-00	动态
10.124.8.87	00-1b-fc-9a-a4-00	动态
10.255.255.255	ff-ff-ff-ff-ff-ff	静态
169.254.169.254	00-1b-fc-9a-a4-00	动态
192.168.0.1	5c-d9-98-f1-89-64	静态
224.0.0.22	01-00-5e-00-00-16	静态
224.0.0.251	01-00-5e-00-00-fb	静态
224.0.0.252	01-00-5e-00-00-fc	静态
239.11.20.1	01-00-5e-0b-14-01	静态
239.255.255.250	01-00-5e-7f-ff-fa	静态
255.255.255.255	ff-ff-ff-ff-ff-ff	静态

## □ Troubleshooting

你可能会在实作三的操作中得到 "ARP 项添加失败: 请求的操作需要提升" 这样的信息, 表示命令没能执行成功, 你该如何解决?

进入管理员模式, 输入\*\*netsh i i show in\*\* 先找出当前的网卡 idx 号。(管理员模式: 电脑左下角“开始”按钮右键, 点击“Windows PowerShell(管理员) (A)” 或者 进入 C 盘 windows\system32 文件夹找到 cmd.exe, 右键“以管理员身份运行”) 然后运行: netsh -c i i add neighbors “idx” “ip 地址” “物理地址”

## 🔧 问题

在实作三中, 为何缓存中常常有网关的信息?

不再同一个子网的 ip 需要经过网关

我们将网关或其它计算机的 arp 信息设置为静态有什么优缺点?

优点: 不容易被 arp 欺骗 安全性较高

缺点: 更换要手动设置 arp 灵活性不高

## 第 8 题 DHCP

【实验过程】(步骤、记录、数据、程序等)

实作一

ipconfig/renew

### Windows IP 配置

不能在 cfw-tap 上执行任何操作, 它已断开媒体连接。

不能在 以太网 2 上执行任何操作, 它已断开媒体连接。

不能在 本地连接\* 2 上执行任何操作, 它已断开媒体连接。

不能在 本地连接\* 3 上执行任何操作, 它已断开媒体连接。

不能在 以太网 上执行任何操作, 它已断开媒体连接。

不能在 WLAN 上执行任何操作, 它已断开媒体连接。

以太网适配器 SSTAP 1:

媒体状态 .....: 媒体已断开连接

连接特定的 DNS 后缀 .....

以太网适配器 cfw-tap:

媒体状态 .....: 媒体已断开连接  
连接特定的 DNS 后缀 .....

未知适配器 aioCloud:

媒体状态 .....: 媒体已断开连接  
连接特定的 DNS 后缀 .....

以太网适配器 以太网 4:

媒体状态 .....: 媒体已断开连接  
连接特定的 DNS 后缀 .....

以太网适配器 以太网 2:

媒体状态 .....: 媒体已断开连接  
连接特定的 DNS 后缀 .....

无线局域网适配器 本地连接\* 2:

媒体状态 .....: 媒体已断开连接  
连接特定的 DNS 后缀 .....

无线局域网适配器 本地连接\* 3:

媒体状态 .....: 媒体已断开连接  
连接特定的 DNS 后缀 .....

以太网适配器 以太网 5:

媒体状态 .....: 媒体已断开连接  
连接特定的 DNS 后缀 .....

以太网适配器 VMware Network Adapter VMnet8:

连接特定的 DNS 后缀 .....:  
本地链接 IPv6 地址.....: fe80::3d3a:5628:ff69:5914%9  
默认网关.....:

以太网适配器 以太网:

媒体状态 .....: 媒体已断开连接  
连接特定的 DNS 后缀 .....

以太网适配器 以太网 3:

连接特定的 DNS 后缀 .....:  
本地链接 IPv6 地址.....: fe80::70b4:de9d:5872:2a37%4  
默认网关.....:

以太网适配器 VMware Network Adapter VMnet1:

连接特定的 DNS 后缀 .....:  
本地链接 IPv6 地址.....: fe80::f42b:238c:56a2:ad20%33  
默认网关.....:

无线局域网适配器 WLAN:

媒体状态 .....: 媒体已断开连接  
连接特定的 DNS 后缀 .....

ipconfig/renew

Windows IP 配置

不能在 SSTAP 1 上执行任何操作，它已断开媒体连接。  
不能在 cfw-tap 上执行任何操作，它已断开媒体连接。  
不能在 aioCloud 上执行任何操作，它已断开媒体连接。  
不能在 以太网 4 上执行任何操作，它已断开媒体连接。  
不能在 以太网 2 上执行任何操作，它已断开媒体连接。  
不能在 本地连接\* 2 上执行任何操作，它已断开媒体连接。  
不能在 本地连接\* 3 上执行任何操作，它已断开媒体连接。  
不能在 以太网 5 上执行任何操作，它已断开媒体连接。  
不能在 以太网 上执行任何操作，它已断开媒体连接。  
不能在 WLAN 上执行任何操作，它已断开媒体连接。

以太网适配器 SSTAP 1:

媒体状态 .....: 媒体已断开连接  
连接特定的 DNS 后缀 .....

以太网适配器 cfw-tap:

媒体状态 .....: 媒体已断开连接  
连接特定的 DNS 后缀 .....

未知适配器 aioCloud:

媒体状态 .....: 媒体已断开连接  
连接特定的 DNS 后缀 .....

以太网适配器 以太网 4:

媒体状态 .....: 媒体已断开连接  
连接特定的 DNS 后缀 .....

以太网适配器 以太网 2:

媒体状态 .....: 媒体已断开连接  
连接特定的 DNS 后缀 .....

无线局域网适配器 本地连接\* 2:

媒体状态 .....: 媒体已断开连接  
连接特定的 DNS 后缀 .....

无线局域网适配器 本地连接\* 3:

媒体状态 .....: 媒体已断开连接  
连接特定的 DNS 后缀 .....

以太网适配器 以太网 5:

媒体状态 .....: 媒体已断开连接  
连接特定的 DNS 后缀 .....

以太网适配器 VMware Network Adapter VMnet8:

连接特定的 DNS 后缀 .....:  
本地链接 IPv6 地址.....: fe80::3d3a:5628:ff69:5914%9  
IPv4 地址 .....: 192.168.222.1  
子网掩码 .....: 255.255.255.0  
默认网关.....:

以太网适配器 以太网:

媒体状态 .....: 媒体已断开连接  
连接特定的 DNS 后缀 .....

以太网适配器 以太网 3:

连接特定的 DNS 后缀 .....:  
本地链接 IPv6 地址.....: fe80::70b4:de9d:5872:2a37%4  
IPv4 地址 .....: 10.125.68.126  
子网掩码 .....: 255.0.0.0  
默认网关.....: 10.125.68.127

以太网适配器 VMware Network Adapter VMnet1:

连接特定的 DNS 后缀 .....:  
本地链接 IPv6 地址.....: fe80::f42b:238c:56a2:ad20%33  
IPv4 地址 .....: 192.168.145.1  
子网掩码 .....: 255.255.255.0  
默认网关.....:

无线局域网适配器 WLAN:

媒体状态 .....: 媒体已断开连接  
连接特定的 DNS 后缀 .....:

## 第 9 题 netstat

【实验过程】（步骤、记录、数据、程序等）

实作一

Windows 系统 将 一 些 常 用 的 端 口 与 服 务 记 录 在 C:\WINDOWS\system32\drivers\etc\services 文件中，请查看该文件了解常用的端口号分配。

```
#
# Format:
#
# <service name> <port number>/<protocol> [aliases...] [#<comment>]
#
```

```
echo          7/tcp
echo          7/udp
discard       9/tcp  sink null
discard       9/udp  sink null
systat        11/tcp  users      #Active users
systat        11/udp  users      #Active users
daytime       13/tcp
daytime       13/udp
qotd          17/tcp  quote      #Quote of the day
qotd          17/udp  quote      #Quote of the day
chargen       19/tcp  ttytst source #Character generator
chargen       19/udp  ttytst source #Character generator
ftp-data      20/tcp
ftp           21/tcp  #FTP. control
ssh           22/tcp  #SSH Remote Login Protocol
telnet        23/tcp
smtp          25/tcp  mail       #Simple Mail Transfer Protocol
time          37/tcp  timserver
time          37/udp  timserver
rlp           39/udp  resource   #Resource Location Protocol
nameserver    42/tcp  name       #Host Name Server
nameserver    42/udp  name       #Host Name Server
nicname       43/tcp  whois
domain        53/tcp
domain        53/udp  #Domain Name Server
```

---

## 实作二

使用 `netstat -an` 命令，查看计算机当前的网络连接状况。更多的 `netstat` 命令选项，可参考上面链接 4 和 5。

## 截取的部分

TCP	0.0.0.0:49665	0.0.0.0:0	LISTENING
TCP	0.0.0.0:49666	0.0.0.0:0	LISTENING
TCP	0.0.0.0:49667	0.0.0.0:0	LISTENING
TCP	0.0.0.0:49668	0.0.0.0:0	LISTENING
TCP	0.0.0.0:49673	0.0.0.0:0	LISTENING
TCP	0.0.0.0:49681	0.0.0.0:0	LISTENING
TCP	10.102.127.240:139	0.0.0.0:0	LISTENING
TCP	10.102.127.240:50074	221.178.10.210:80	CLOSE_WAIT



TCP	10.102.127.240:50797	221.178.101.24:443	CLOSE_WAIT
TCP	10.102.127.240:51099	120.253.253.225:443	TIME_WAIT
TCP	10.102.127.240:52239	218.201.40.58:443	ESTABLISHED
TCP	10.102.127.240:53306	120.241.186.232:443	CLOSE_WAIT
TCP	10.102.127.240:53307	120.241.186.232:443	CLOSE_WAIT
TCP	10.102.127.240:53308	120.241.186.232:443	CLOSE_WAIT
TCP	10.102.127.240:53313	121.51.142.35:443	CLOSE_WAIT
TCP	10.102.127.240:53335	120.241.186.231:443	CLOSE_WAIT
TCP	10.102.127.240:54241	13.78.60.116:51519	CLOSE_WAIT
TCP	10.102.127.240:57886	183.230.77.224:443	CLOSE_WAIT
TCP	10.102.127.240:58068	52.139.250.253:443	ESTABLISHED
TCP	10.102.127.240:59500	13.78.60.116:51519	ESTABLISHED
TCP	10.102.127.240:59524	13.89.179.10:443	TIME_WAIT
TCP	10.102.127.240:59881	36.155.229.173:80	ESTABLISHED
TCP	10.102.127.240:59899	120.241.186.232:443	CLOSE_WAIT
TCP	10.102.127.240:61267	112.64.218.40:80	CLOSE_WAIT
TCP	10.102.127.240:62475	13.78.60.116:51519	TIME_WAIT
TCP	10.102.127.240:62640	13.78.60.116:51519	ESTABLISHED
TCP	10.102.127.240:63807	13.78.60.116:51519	ESTABLISHED
TCP	10.102.127.240:64657	112.60.13.243:443	CLOSE_WAIT
TCP	127.0.0.1:4301	0.0.0.0	LISTENING
TCP	127.0.0.1:7470	127.0.0.1:54891	ESTABLISHED

## 第 10 题 DNS

【实验过程】（步骤、记录、数据、程序等）

实作一

Windows 系统 将 一些 固 定 的 / 静 态 的 DNS 信 息 记 录 在 C:\WINDOWS\system32\drivers\etc\hosts 文 件 中，如 我 们 常 用 的 localhost 就 对 应 127.0.0.1 。请 查 看 该 文 件 看 看 有 什 么 记 录 在 该 文 件 中。

```
# Copyright (c) 1993-2009 Microsoft Corp.
```

```
#
```

```
# This is a sample HOSTS file used by Microsoft TCP/IP for Windows.
```

```
#
```

```
# This file contains the mappings of IP addresses to host names. Each
```

```
# entry should be kept on an individual line. The IP address should
```

```
# be placed in the first column followed by the corresponding host name.
```

```
# The IP address and the host name should be separated by at least one
```

```
# space.
```

```
#
```

```
# Additionally, comments (such as these) may be inserted on individual
```

```
# lines or following the machine name denoted by a '#' symbol.
```

```
#
```

```
# For example:
```

```
#
#      102.54.94.97      rhino.acme.com      # source server
#      38.25.63.10      x.acme.com          # x client host
# localhost name resolution is handled within DNS itself.
# 127.0.0.1      localhost
# ::1            localhost

127.0.0.1      activate.navicat.com
```

## 实作二

解析过的 DNS 记录将会被缓存，以利于加快解析速度。请使用 `ipconfig /displaydns` 命令查看。我们也可以使用 `ipconfig /flushdns` 命令来清除所有的 DNS 缓存。

```
honor_9x-cca6923357298178.mshome.net
```

```
-----
没有 AAAA 类型的记录
```

```
honor_9x-cca6923357298178.mshome.net
```

```
-----
记录名称.....: HONOR_9X-cca6923357298178.mshome.net
记录类型.....: 1
生存时间.....: 601817
数据长度.....: 4
部分.....: 答案
A (主机)记录  ....: 192.168.137.72
```

```
1.0.0.127.in-addr.arpa
```

```
-----
记录名称.....: 1.0.0.127.in-addr.arpa.
记录类型.....: 12
生存时间.....: 601817
数据长度.....: 8
部分.....: 答案
PTR 记录  ....: activate.navicat.com
```

```
beacons.gcp.gvt2.com
```

```
-----
记录名称.....: beacons.gcp.gvt2.com
记录类型.....: 1
```

生存时间.....: 898  
数据长度.....: 4  
部分.....: 答案  
A (主机)记录 .....: 0.0.0.0

www.my-cybercafe.de

-----  
记录名称.....: www.my-cybercafe.de  
记录类型.....: 1  
生存时间.....: 2154  
数据长度.....: 4  
部分.....: 答案  
A (主机)记录 .....: 109.237.134.14

desktop-lf4p0s5.mshome.net

-----  
没有 AAAA 类型的记录

desktop-lf4p0s5.mshome.net

-----  
记录名称.....: DESKTOP-LF4P0S5.mshome.net  
记录类型.....: 1  
生存时间.....: 601817  
数据长度.....: 4  
部分.....: 答案  
A (主机)记录 .....: 192.168.137.1

158.137.168.192.in-addr.arpa

-----  
记录名称.....: 158.137.168.192.in-addr.arpa.  
记录类型.....: 12  
生存时间.....: 601817  
数据长度.....: 8  
部分.....: 答案  
PTR 记录 .....: M2010J19SC-219531107.mshome.net

down.verify.stat.xunlei.com

-----  
记录名称.....: down.verify.stat.xunlei.com

记录类型.....: 1  
生存时间.....: 1362  
数据长度.....: 4  
部分.....: 答案  
A (主机)记录 ....: 127.0.0.1

1.137.168.192.in-addr.arpa

-----  
记录名称.....: 1.137.168.192.in-addr.arpa.  
记录类型.....: 12  
生存时间.....: 601817  
数据长度.....: 8  
部分.....: 答案  
PTR 记录 .....: DESKTOP-LF4P0S5.mshome.net

72.137.168.192.in-addr.arpa

-----  
记录名称.....: 72.137.168.192.in-addr.arpa.  
记录类型.....: 12  
生存时间.....: 601817  
数据长度.....: 8  
部分.....: 答案  
PTR 记录 .....: HONOR\_9X-cca6923357298178.mshome.net

avatars.githubusercontent.com

-----  
记录名称.....: avatars.githubusercontent.com  
记录类型.....: 1  
生存时间.....: 1982  
数据长度.....: 4  
部分.....: 答案  
A (主机)记录 ....: 185.199.110.133

记录名称.....: avatars.githubusercontent.com  
记录类型.....: 1  
生存时间.....: 1982  
数据长度.....: 4  
部分.....: 答案  
A (主机)记录 ....: 185.199.111.133

记录名称.....: avatars.githubusercontent.com  
记录类型.....: 1  
生存时间.....: 1982  
数据长度.....: 4  
部分.....: 答案  
A (主机)记录 ....: 185.199.108.133

记录名称.....: avatars.githubusercontent.com  
记录类型.....: 1  
生存时间.....: 1982  
数据长度.....: 4  
部分.....: 答案  
A (主机)记录 ....: 185.199.109.133

activate.navicat.com

-----  
没有 AAAA 类型的记录

activate.navicat.com

-----  
记录名称.....: activate.navicat.com  
记录类型.....: 1  
生存时间.....: 601817  
数据长度.....: 4  
部分.....: 答案  
A (主机)记录 ....: 127.0.0.1

m2010j19sc-219531107.mshome.net

-----  
没有 AAAA 类型的记录

m2010j19sc-219531107.mshome.net

-----  
记录名称.....: M2010J19SC-219531107.mshome.net  
记录类型.....: 1  
生存时间.....: 601817  
数据长度.....: 4  
部分.....: 答案

A (主机)记录 .....: 192.168.137.158

### 实作三

使用 `nslookup qige.io` 命令，将使用默认的 DNS 服务器查询该域名。当然你也可以指定使用 CloudFlare (1.1.1.1) 或 Google (8.8.8.8) 的全球 DNS 服务器来解析，如：  
`nslookup qige.io 8.8.8.8`，当然，由于你懂的原因，这不一定会得到正确的答案。

DNS request timed out.  
timeout was 2 seconds.  
服务器: UnKnown  
Address: 183.230.126.225

DNS request timed out.  
timeout was 2 seconds.  
DNS request timed out.  
timeout was 2 seconds.  
DNS request timed out.  
timeout was 2 seconds.  
DNS request timed out.  
timeout was 2 seconds.  
\*\*\* 请求 UnKnown 超时

### ☐ Troubleshooting

上面秘籍中我们提到了使用插件或自己修改 `hosts` 文件来屏蔽广告，思考一下这种方式为何能过滤广告？如果某些广告拦截失效，那么是什么原因？你应该怎样进行分析从而能够成功屏蔽它？

***hosts 的广告域名解析到空服务器导致广告不能连接到服务器***  
***广告可能是用的多个ip 而不是域名***  
***屏蔽广告服务器的所有ip***

### 第 11 题 cache

【实验过程】（步骤、记录、数据、程序等）

#### 实作一

打开 Chrome 或 Firefox 浏览器，访问 `https://qige.io`，接下来敲 F12 键 或 Ctrl + Shift + I 组合键打开开发者工具，选择 Network 面板后刷新页面，你会在开发者工具底部看到加载该页面花费的时间。请进一步查看哪些文件被 cache 了，哪些没有。



