

---

# CSG1105 Workshop Seven

---

## 1 INTRODUCTION

This week we are going to explore some basic aspects of DHCP(Dynamic Host Configuration Protocol). This protocol is used to automatically configure devices on IP networks. Today we are only looking at simple aspects of the protocol. On complex networks, it may be more comprehensively configured to tailor specific devices.

## 2 EXERCISE: VIEWING DHCP PROTOCOL IN WIRESHARK

Your PC will have a DHCP lease that was obtained when you connected to a network or started your computer. In order to capture the packets exchanged by DHCP Clients and Servers, you will need to force the PC to renew the lease.

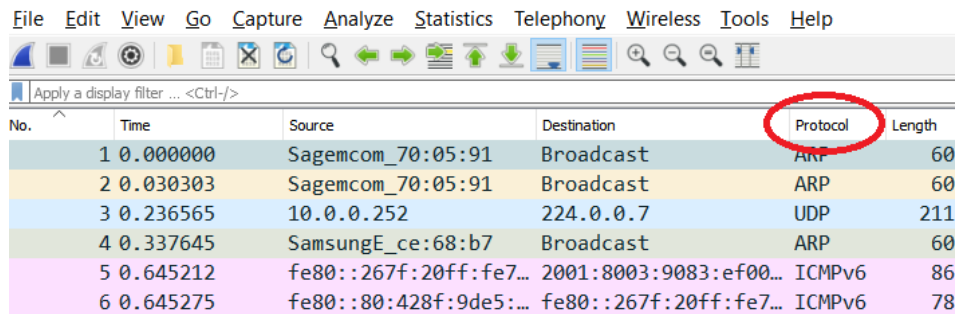
1. Using what you have learnt in previous weeks, check the basic IP information of the PC you're working on. (Hint: either `ipconfig` or `ifconfig` from the command line)
2. Start Wireshark capturing packets on the interface you need to restart

### 2.1 Windows

- a) Open a Windows command prompt. (Win Key + R,type "`cmd`",OK)
- b) Type `ip config /release` to end the DHCP lease
- c) Type `ipconfig /renew` to renew the DHCP lease

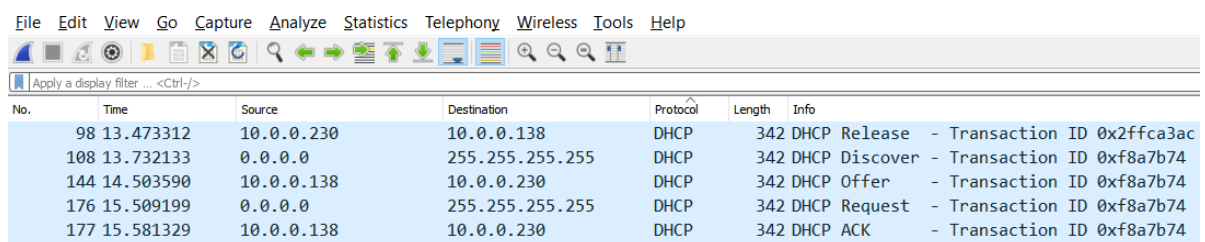
### 2.2 OS X

- a) Use Finder to navigate to Applications->Utilities
  - b) Start the Terminal.app
  - c) Type `sudo ipconfig set en0 DHCP` for Ethernet or `en1` for WiFi (Check your interfaces with `ifconfig`). The `sudo` command runs the following command as the administrator and will require you to enter a password.
3. Stop the Wireshark capture
  4. Click the **Protocol** column header to sort it in alphabetical order



No.	Time	Source	Destination	Protocol	Length
1	0.000000	Sagemcom_70:05:91	Broadcast	ARP	60
2	0.030303	Sagemcom_70:05:91	Broadcast	ARP	60
3	0.236565	10.0.0.252	224.0.0.7	UDP	211
4	0.337645	SamsungE_ce:68:b7	Broadcast	ARP	60
5	0.645212	fe80::267f:20ff:fe7...	2001:8003:9083:ef00...	ICMPv6	86
6	0.645275	fe80::80:428f:9de5:...	fe80::267f:20ff:fe7...	ICMPv6	78

5. Scroll up or down until you see the DHCP messages



No.	Time	Source	Destination	Protocol	Length	Info
98	13.473312	10.0.0.230	10.0.0.138	DHCP	342	DHCP Release - Transaction ID 0x2ffc3ac
108	13.732133	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0xf8a7b74
144	14.503590	10.0.0.138	10.0.0.230	DHCP	342	DHCP Offer - Transaction ID 0xf8a7b74
176	15.509199	0.0.0.0	255.255.255.255	DHCP	342	DHCP Request - Transaction ID 0xf8a7b74
177	15.581329	10.0.0.138	10.0.0.230	DHCP	342	DHCP ACK - Transaction ID 0xf8a7b74

- The first message type (See the Info column) is a **Release** message. This is the Client informing the server that the IP address lease is no longer required.
- The following four packets follow the **DORA** acronym: Discover, Offer, Request and Acknowledgment.
- Select the **Discover** frame
- The source IP is 0.0.0.0 i.e. not set and the destination is 255.255.255.255 i.e. a broadcast that will translate to FF:FF:FF:FF:FF:FF a MAC broadcast.
- Go to Wireshark's middle window and expand the payload, the **Bootstrap Protocol**
- All of the IP addresses are set to 0.0.0.0, the only address set is the Client MAC address

#### Bootstrap Protocol (Discover)

```

Message type:  Boot Request (1)
Hardware type:  Ethernet (0x01)
Hardware address length:  6
Hops:  0
Transaction ID:  0x0f8a7b74
Seconds elapsed:  0
>Bootp flags:  0x0000 (Unicast)
Client IP address:  0.0.0.0
Your (client) IP address:  0.0.0.0
Next server IP address:  0.0.0.0
Relay agent IP address:  0.0.0.0
Client MAC address:  Apple_d0:85:1e (78:7b:8a:d0:85:1e)
Client hardware address padding:  00000000000000000000
Server host name not given
Boot file name not given
Magic cookie:  DHCP
>Option:  (53) DHCP Message Type (Discover)
>Option:  (55) Parameter Request List

```

```
>Option: (57) Maximum DHCP Message Size
>Option: (61) Client identifier
>Option: (51) IP Address Lease Time
>Option: (12) Host Name
>Option: (255) End
Padding: 00000000000000000000
```

12. A list of available options and their definitions may be found in <https://tools.ietf.org/html/rfc2132>
13. Now select the **Offer** packet. We can see some new information appears, focusing only on the client relevant information:  
 DHCP Server Identifier - the IP address of the DHCP server  
 IP Address Lease Time - how long the IP address will be assigned before another DHCP communication will take place  
 Subnet Mask - the subnet mask of the network  
 DomainName - the domain, also called 'workgroup'  
 Router - the default gateway of the network  
 Domain Name Server - the address of where website addresses can be translated into IP addresses
14. Now select the **Request** packet. In the DHCP Request we can see that the client (workstation) confirms some of the information and relays back its information such as its identifier and its own domain name.
15. Now select the DHCP ACK packet. We can see that the server has made no modifications and the workstation understands that it now has its assigned IP address for all communications.
16. Take some time to expand each of the subfields of the four packets and examine the values. Relate what you're seeing in the fields with the configuration of your machine.
17. **Note:** Some of the fields and broadcasts may be different on your machine as there are unique features to all networks and operating systems.

### 3 SUMMARY

In this workshop, we have built on the previous exercises in Wireshark to look at a particular protocol, DHCP. There is much more to DHCP than we have had time to cover. To understand more about DHCP, read section 3.7 in [Parziale et al] Parziale, Lydia et al, 2006, *TCP/IP Tutorial and Technical Overview*, IBM, Poughkeepsie, NY, retrieved from:  
<http://www.redbooks.ibm.com/redbooks/pdfs/gg243376.pdf>