California State University, Monterey Bay

Week 6 – Lab 6
Group 10

Clarence Mitchell

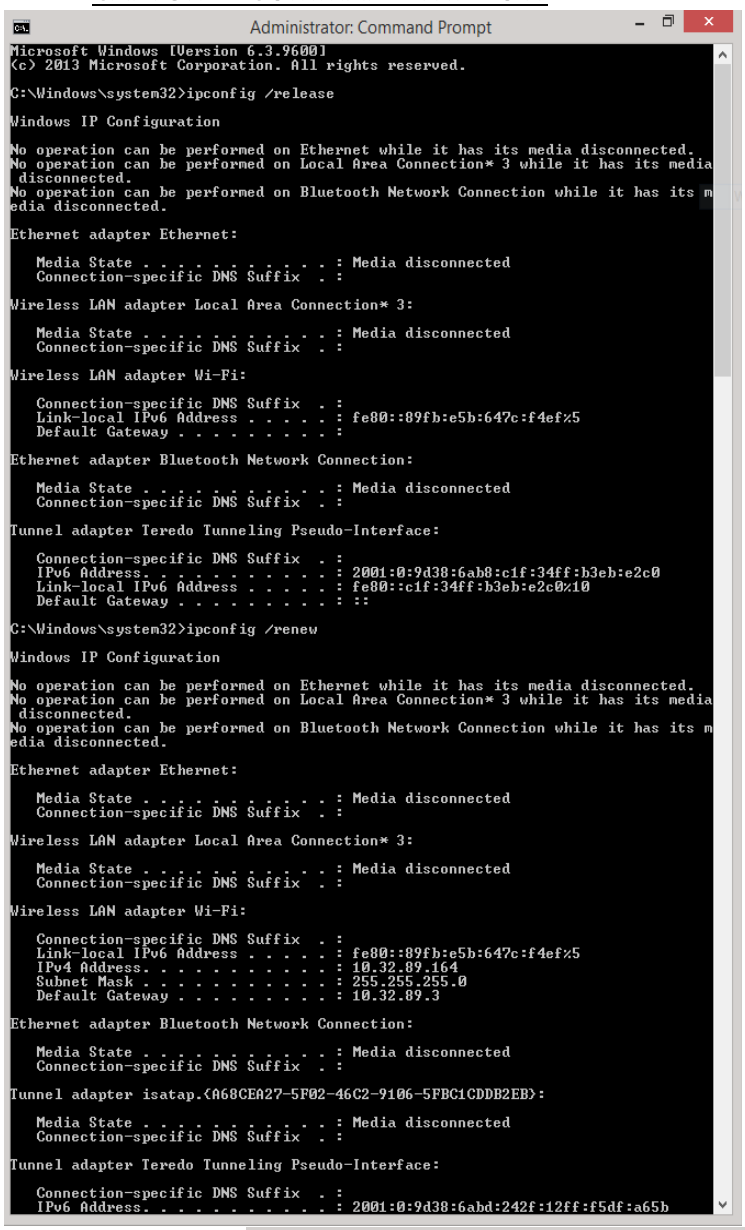
CST311

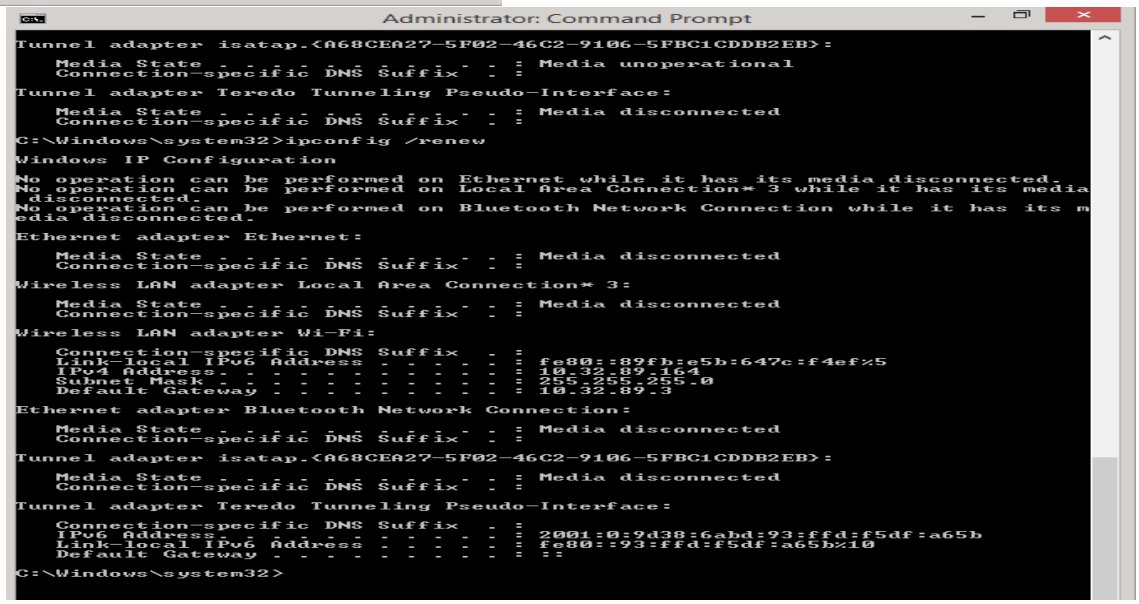
Introduction to Computer Networks

SUMMER 2015

Instructor: Dr. Anand Seetharam

CAPTURED COMMAND WINDOW



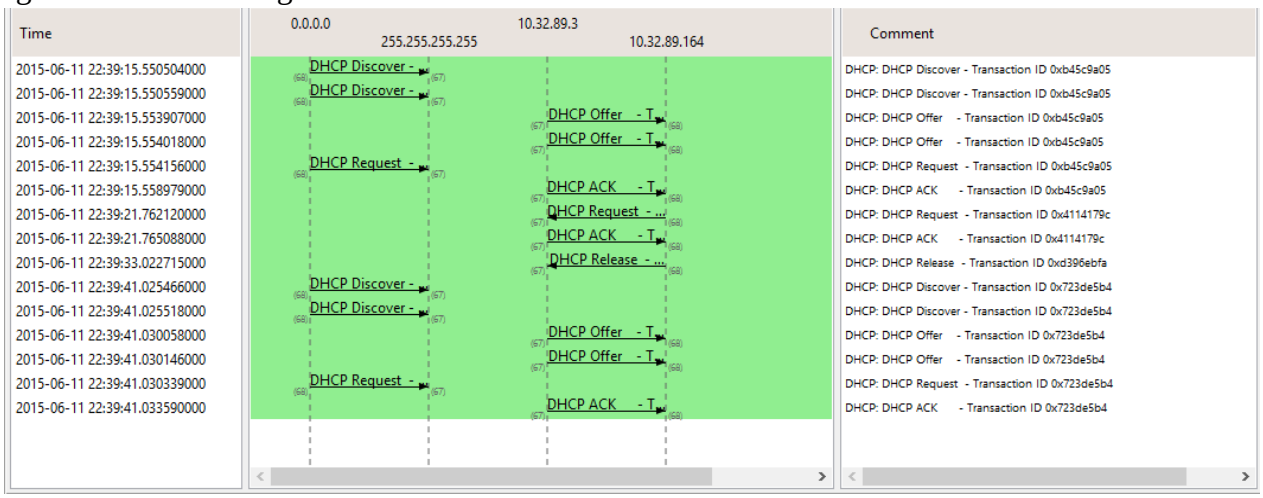


1. Are DHCP messages sent over UDP or TCP?

```
Frame 360: 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits) on interface 0
Ethernet II, Src: HonHaiPr_62:0a:cb (ac:d1:b8:62:0a:cb), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
Internet Protocol Version 4, Src: 0.0.0.0 (0.0.0.0), Dst: 255.255.255.255 (255.255.255.255)
User Datagram Protocol, Src Port: 68 (68), Dst Port: 67 (67)
    Source Port: 68 (68)
    Destination Port: 67 (67)
    Length: 308
  Checksum: 0x1b6a [validation disabled]
    [Stream index: 148]
Bootstrap Protocol (Discover)
```

- DHCP messages are sent over UDP.

2. Draw a timing datagram illustrating the sequence of the first four-packet Discover/Offer/Request/ACK DHCP exchange between the client and server. For each packet, indicated the source and destination port numbers. Are the port numbers the same as in the example given in this lab assignment?



. The port numbers are the same as the example in the Lab.

3. What is the link-layer (e.g., Ethernet) address of your host?
   - The Link Layer address of my workstation is: ac:d1:b8:62:0a:cb..

```
Frame 360: 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits) on interface 0
Ethernet II, Src: HonHaiPr_62:0a:cb (ac:d1:b8:62:0a:cb), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
Internet Protocol Version 4, Src: 0.0.0.0 (0.0.0.0), Dst: 255.255.255.255 (255.255.255.255)
User Datagram Protocol, Src Port: 68 (68), Dst Port: 67 (67)
    Source Port: 68 (68)
    Destination Port: 67 (67)
    Length: 308
  Checksum: 0x1b6a [validation disabled]
    [Stream index: 148]
Bootstrap Protocol (Discover)
```

4. What values in the DHCP discover message differentiate this message from the DHCP request message?
   - The values which differentiate the Discover message from the Request message are in “Option 53: DHCP Message Type”..

360	2015-06-11 22:39:15.550504000	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0xb45c9a05
361	2015-06-11 22:39:15.550559000	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0xb45c9a05
366	2015-06-11 22:39:15.553907000	10.32.89.3	10.32.89.164	DHCP	342	DHCP Offer - Transaction ID 0xb45c9a05
367	2015-06-11 22:39:15.554018000	10.32.89.3	10.32.89.164	DHCP	342	DHCP Offer - Transaction ID 0xb45c9a05
368	2015-06-11 22:39:15.554156000	0.0.0.0	255.255.255.255	DHCP	351	DHCP Request - Transaction ID 0xb45c9a05
369	2015-06-11 22:39:15.558979000	10.32.89.3	10.32.89.164	DHCP	348	DHCP ACK - Transaction ID 0xb45c9a05
1786	2015-06-11 22:39:21.762120000	10.32.89.164	10.32.89.3	DHCP	342	DHCP Request - Transaction ID 0x4114179c
1787	2015-06-11 22:39:21.765088000	10.32.89.3	10.32.89.164	DHCP	348	DHCP ACK - Transaction ID 0x4114179c
2224	2015-06-11 22:39:33.022715000	10.32.89.164	10.32.89.3	DHCP	342	DHCP Release - Transaction ID 0xd396ebfa
2416	2015-06-11 22:39:41.025466000	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0x723de5b4
2417	2015-06-11 22:39:41.025518000	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0x723de5b4
2418	2015-06-11 22:39:41.030058000	10.32.89.3	10.32.89.164	DHCP	342	DHCP Offer - Transaction ID 0x723de5b4
2419	2015-06-11 22:39:41.030146000	10.32.89.3	10.32.89.164	DHCP	342	DHCP Offer - Transaction ID 0x723de5b4
2420	2015-06-11 22:39:41.030339000	0.0.0.0	255.255.255.255	DHCP	351	DHCP Request - Transaction ID 0x723de5b4
2421	2015-06-11 22:39:41.033590000	10.32.89.3	10.32.89.164	DHCP	348	DHCP ACK - Transaction ID 0x723de5b4

- .

5. What is the value of the Transaction-ID in each of the first four (Discover/Offer/Request/ACK) DHCP messages? What are the values of the Transaction-ID in the second set (Request/ACK) set of DHCP messages? What is the purpose of the Transaction-ID field?
    - The value of the Transaction ID is 0xb45c9a05. The second Transaction ID is 0x723de5b4. A Transaction ID is used so that the DHCP server can differentiate between client requests during the request process..

6. A host uses DHCP to obtain an IP address, among other things. But a host's IP address is not confirmed until the end of the four-message exchange! If the IP address is not set until the end of the four-message exchange, then what values are used in the IP datagrams in the four-message exchange? For each of the four DHCP messages (Discover/Offer/Request/ACK DHCP), indicate the source and destination IP addresses that are carried in the encapsulating IP datagram.
    - The DHCP client and server both use 255.255.255.255 as the destination address. The client uses source IP address 0.0.0.0, while the server uses its actual IP address as the source...

7. What is the IP address of your DHCP server?
    - The IP address of the DHCP server is 10.32.89.3..

8. What IP address is the DHCP server offering to your host in the DHCP Offer message? Indicate which DHCP message contains the offered DHCP address.
    - The DHCP server offered the IP address 10.32.89.164 to my client machine. The DHCP message with "DHCP Message Type = DHCP Offer" contained the offered IP..

9. In the example screenshot in this assignment, there is no relay agent between the host and the DHCP server. What values in the trace indicate the absence of a relay agent? Is there a relay agent in your experiment? If so what is the IP address of the agent?
    - The "Relay agent IP address" is 0.0.0.0, which indicates that there is no DHCP Relay used. There was no Relay Agent used in my experiment..

```
Hops: 0
Transaction ID: 0xb45c9a05
Seconds elapsed: 0
⊟ Bootp flags: 0x0000 (Unicast)
    0... .... .... .... = Broadcast flag: Unicast
    .000 0000 0000 0000 = Reserved flags: 0x0000
Client IP address: 0.0.0.0 (0.0.0.0)
Your (client) IP address: 0.0.0.0 (0.0.0.0)
Next server IP address: 0.0.0.0 (0.0.0.0)
Relay agent IP address: 0.0.0.0 (0.0.0.0)
Client MAC address: HonHaiPr_62:0a:cb (ac:d1:b8:62:0a:cb)
Client hardware address padding: 00000000000000000000
Server host name not given
Boot file name not given
Magic cookie: DHCP
⊟ Option: (53) DHCP Message Type (Discover)
    Length: 1
```

10. Explain the purpose of the router and subnet mask lines in the DHCP offer message.
    - The router line indicates to the client what its default gateway should be. The subnet mask line tells the client which subnet mask it should use...

11. In the DHCP trace file noted in footnote 2, the DHCP server offers a specific IP address to the client (see also question 8. above). In the client's response to the first server OFFER message, does the client accept this IP address? Where in the client's RESPONSE is the client's requested address?
    - In my experiment, the host requests the offered IP address in the DHCP Request message...

```
⊞ Frame 368: 351 bytes on wire (2808 bits), 351 bytes captured (2808 bits) on interface 0
⊞ Ethernet II, Src: HonHaiPr_62:0a:cb (ac:d1:b8:62:0a:cb), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
⊞ Internet Protocol Version 4, Src: 0.0.0.0 (0.0.0.0), Dst: 255.255.255.255 (255.255.255.255)
⊞ User Datagram Protocol, Src Port: 68 (68), Dst Port: 67 (67)
⊟ Bootstrap Protocol (Request)
    Message type: Boot Request (1)
    Hardware type: Ethernet (0x01)
    Hardware address length: 6
    Hops: 0
    Transaction ID: 0xb45c9a05
    Seconds elapsed: 0
  ⊞ Bootp flags: 0x0000 (Unicast)
    Client IP address: 0.0.0.0 (0.0.0.0)
    Your (client) IP address: 0.0.0.0 (0.0.0.0)
    Next server IP address: 0.0.0.0 (0.0.0.0)
    Relay agent IP address: 0.0.0.0 (0.0.0.0)
    Client MAC address: HonHaiPr_62:0a:cb (ac:d1:b8:62:0a:cb)
    Client hardware address padding: 00000000000000000000
    Server host name not given
    Boot file name not given
    Magic cookie: DHCP
  ⊞ Option: (53) DHCP Message Type (Request)
  ⊞ Option: (61) Client identifier
  ⊟ Option: (50) Requested IP Address
      Length: 4
      Requested IP Address: 10.32.89.164 (10.32.89.164)
  ⊞ Option: (54) DHCP Server Identifier
  ⊞ Option: (12) Host Name
  ⊟ Option: (81) Client Fully Qualified Domain Name
```

12. Explain the purpose of the lease time. How long is the lease time in your experiment?
    - The lease time is the amount of time the DHCP server assigns an IP address to a client. During the lease time, the DHCP server will not assign the IP given to the client to another client, unless it is released by the client. Once the lease time has expired, the IP address can be reused by the DHCP server to give to another client. In my experiment, the lease time is 1 day.

13. What is the purpose of the DHCP release message? Does the DHCP server issue an acknowledgment of receipt of the client's DHCP request? What would happen if the client's DHCP release message is lost?
    - The client sends a DHCP Release message to cancel its lease on the IP address given to it by the DHCP server. The DHCP server does not send a message back to the client acknowledging the DHCP Release message. If the DHCP Release message from the client is lost, the DHCP server would have to wait until the lease period is over for that IP address until it could reuse it for another client..

14. Clear the *bootp* filter from your Wireshark window. Were any ARP packets sent or received during the DHCP packet-exchange period? If so, explain the purpose of those ARP packets.

    - Yes, there are ARP requests made by the DHCP server. Before offering an IP address to a client, the DHCP server issues an ARP request for the offered IP to make sure the IP address is not already in use by another workstation.