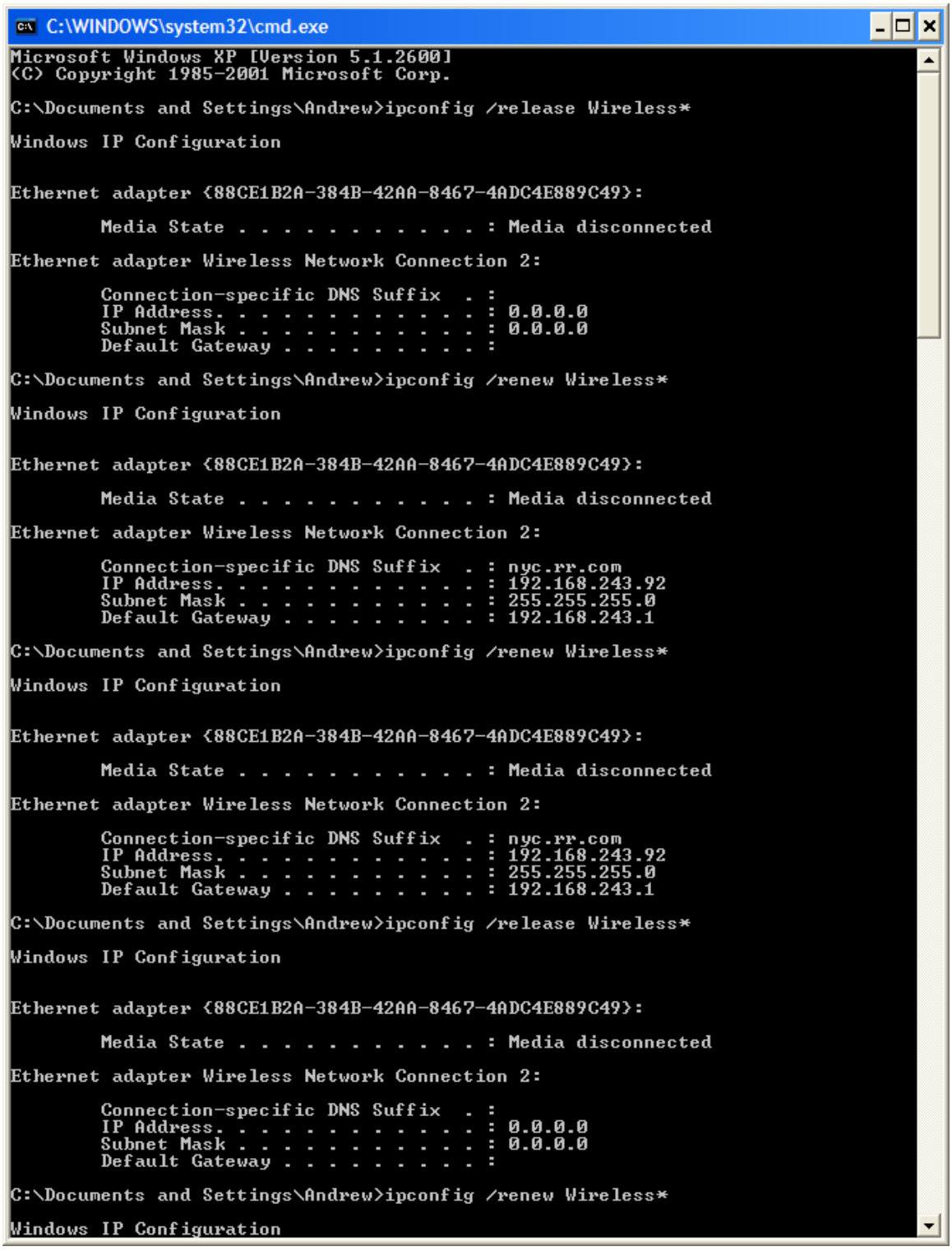
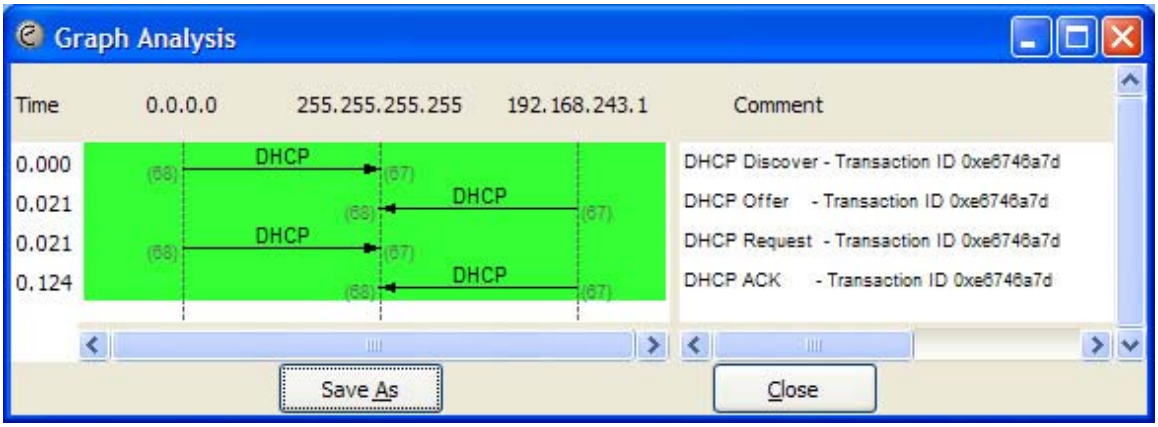
Wireshark Lab Solution: DHCP



1. DHCP messages are sent over UDP (User Datagram Protocol).

```
Frame 2 (342 bytes on wire, 342 bytes captured)
Ethernet II, Src: 192.168.243.92 (00:90:4b:69:dd:34), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
Internet Protocol, Src: 0.0.0.0 (0.0.0.0), Dst: 255.255.255.255 (255.255.255.255)
User Datagram Protocol, Src Port: bootpc (68), Dst Port: bootps (67)
    Source port: bootpc (68)
    Destination port: bootps (67)
    Length: 308
    Checksum: 0xd1a1 [correct]
Bootstrap Protocol
```

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



3. The Link Layer address of my workstation is: 00:90:4b:69:dd:34

```
Frame 1 (342 bytes on wire, 342 bytes captured)
Ethernet II, Src: 192.168.243.92 (00:90:4b:69:dd:34), Dst: Broadcast
(ff:ff:ff:ff:ff:ff)
    Destination: Broadcast (ff:ff:ff:ff:ff:ff)
    Source: 192.168.243.92 (00:90:4b:69:dd:34)
    Type: IP (0x0800)
Internet Protocol, Src: 0.0.0.0 (0.0.0.0), Dst: 255.255.255.255 (255.255.255.255)
User Datagram Protocol, Src Port: bootpc (68), Dst Port: bootps (67)
Bootstrap Protocol
```

4. The values which differentiate the Discover message from the Request message are in “Option 53: DHCP Message Type”.

```
Frame 1 (342 bytes on wire, 342 bytes captured)
Ethernet II, Src: 192.168.243.92 (00:90:4b:69:dd:34), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
Internet Protocol, Src: 0.0.0.0 (0.0.0.0), Dst: 255.255.255.255 (255.255.255.255)
User Datagram Protocol, Src Port: bootpc (68), Dst Port: bootps (67)
Bootstrap Protocol
    Message type: Boot Request (1)
    Hardware type: Ethernet
    Hardware address length: 6
    Hops: 0
    Transaction ID: 0xe6746a7d
    Seconds elapsed: 1280
    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: 192.168.243.92 (00:90:4b:69:dd:34)
    Server host name not given
    Boot file name not given
    Magic cookie: (OK)
    Option 53: DHCP Message Type = DHCP Discover
    Option 116: DHCP Auto-Configuration (1 bytes)
    Option 61: Client identifier
    Option 50: Requested IP Address = 192.168.243.92
    Option 12: Host Name = "homelt"
    Option 60: Vendor class identifier = "MSFT 5.0"
    Option 55: Parameter Request List
    End Option
    Padding

Frame 3 (350 bytes on wire, 350 bytes captured)
Ethernet II, Src: 192.168.243.92 (00:90:4b:69:dd:34), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
Internet Protocol, Src: 0.0.0.0 (0.0.0.0), Dst: 255.255.255.255 (255.255.255.255)
User Datagram Protocol, Src Port: bootpc (68), Dst Port: bootps (67)
Bootstrap Protocol
    Message type: Boot Request (1)
    Hardware type: Ethernet
    Hardware address length: 6
    Hops: 0
    Transaction ID: 0xe6746a7d
    Seconds elapsed: 1280
    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: 192.168.243.92 (00:90:4b:69:dd:34)
    Server host name not given
    Boot file name not given
    Magic cookie: (OK)
    Option 53: DHCP Message Type = DHCP Request
    Option 61: Client identifier
    Option 50: Requested IP Address = 192.168.243.92
    Option 54: Server Identifier = 192.168.243.1
    Option 12: Host Name = "homelt"
    Option 81: FQDN
    Option 60: Vendor class identifier = "MSFT 5.0"
    Option 55: Parameter Request List
    End Option
```

5. The value of the Transaction ID is 0xe6746a7d. The second Transaction ID is 0xe4eff25f. A Transaction ID is used so that the DHCP server can differentiate between client requests during the request process.

```
No.     Time        Source                Destination           Protocol Info
      3 5.000175    0.0.0.0               255.255.255.255       DHCP     DHCP Discover - Transaction ID 0xe6746a7d
     27 12.075229   192.168.243.92        192.168.243.1         DHCP     DHCP Request  - Transaction ID 0xe4eff25f
```

6. 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.

```
No.     Time        Source                Destination           Protocol Info
      1 0.000000    0.0.0.0               255.255.255.255       DHCP     DHCP Discover - Transaction ID 0xe6746a7d
      2 0.020995    192.168.243.1         255.255.255.255       DHCP     DHCP Offer    - Transaction ID 0xe6746a7d
      3 0.021346    0.0.0.0               255.255.255.255       DHCP     DHCP Request  - Transaction ID 0xe6746a7d
      4 0.124018    192.168.243.1         255.255.255.255       DHCP     DHCP ACK      - Transaction ID 0xe6746a7d
```

7. The IP address of the DHCP server is 192.168.243.1

```
No.     Time        Source                Destination           Protocol Info
      4 0.124018    192.168.243.1         255.255.255.255       DHCP     DHCP ACK      - Transaction ID 0xe6746a7d
```

8. The DHCP server offered the IP address 192.168.243.92 to my client machine. The DHCP message with “DHCP Message Type = DHCP Offer” contained the offered IP.

```
Frame 2 (590 bytes on wire, 590 bytes captured)
Ethernet II, Src: 192.168.243.1 (00:08:da:50:49:c5), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
Internet Protocol, Src: 192.168.243.1 (192.168.243.1), Dst: 255.255.255.255 (255.255.255.255)
User Datagram Protocol, Src Port: bootps (67), Dst Port: bootpc (68)
Bootstrap Protocol
    Message type: Boot Reply (2)
    Hardware type: Ethernet
    Hardware address length: 6
    Hops: 0
    Transaction ID: 0xe6746a7d
    Seconds elapsed: 1280
    Bootp flags: 0x0000 (Unicast)
    Client IP address: 0.0.0.0 (0.0.0.0)
    Your (client) IP address: 192.168.243.92 (192.168.243.92)
    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: 192.168.243.92 (00:90:4b:69:dd:34)
    Server host name not given
    Boot file name not given
    Magic cookie: (OK)
    Option 53: DHCP Message Type = DHCP Offer
    Option 1: Subnet Mask = 255.255.255.0
    Option 54: Server Identifier = 192.168.243.1
    Option 51: IP Address Lease Time = 3 days
    Option 6: Domain Name Server = 192.168.243.1
    Option 5: Name Server = 24.29.103.10
    Option 15: Domain Name = "nyc.rr.com"
    Option 31: Perform Router Discover = Enabled
    End Option
    Padding
```

9. 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.

```
Frame 4 (590 bytes on wire, 590 bytes captured)
Ethernet II, Src: 192.168.243.1 (00:08:da:50:49:c5), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
Internet Protocol, Src: 192.168.243.1 (192.168.243.1), Dst: 255.255.255.255 (255.255.255.255)
User Datagram Protocol, Src Port: bootps (67), Dst Port: bootpc (68)
Bootstrap Protocol
    Message type: Boot Reply (2)
    Hardware type: Ethernet
    Hardware address length: 6
    Hops: 0
    Transaction ID: 0xe6746a7d
    Seconds elapsed: 1280
    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: 192.168.243.92 (192.168.243.92)
    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: 192.168.243.92 (00:90:4b:69:dd:34)
    Server host name not given
    Boot file name not given
    Magic cookie: (OK)
    Option 53: DHCP Message Type = DHCP ACK
    Option 54: Server Identifier = 192.168.243.1
    Option 51: IP Address Lease Time = 3 days
    Option 1: Subnet Mask = 255.255.255.0
    Option 3: Router = 192.168.243.1
    Option 6: Domain Name Server = 192.168.243.1
    Option 5: Name Server = 24.29.103.10
    Option 15: Domain Name = "nyc.rr.com"
    Option 31: Perform Router Discover = Enabled
    End Option
```

10. 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.

```
Frame 4 (590 bytes on wire, 590 bytes captured)
Ethernet II, Src: 192.168.243.1 (00:08:da:50:49:c5), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
Internet Protocol, Src: 192.168.243.1 (192.168.243.1), Dst: 255.255.255.255 (255.255.255.255)
User Datagram Protocol, Src Port: bootps (67), Dst Port: bootpc (68)
Bootstrap Protocol
    Message type: Boot Reply (2)
    Hardware type: Ethernet
    Hardware address length: 6
    Hops: 0
    Transaction ID: 0xe6746a7d
    Seconds elapsed: 1280
    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: 192.168.243.92 (192.168.243.92)
    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: 192.168.243.92 (00:90:4b:69:dd:34)
    Server host name not given
    Boot file name not given
    Magic cookie: (OK)
    Option 53: DHCP Message Type = DHCP ACK
    Option 54: Server Identifier = 192.168.243.1
    Option 51: IP Address Lease Time = 3 days
    Option 1: Subnet Mask = 255.255.255.0
    Option 3: Router = 192.168.243.1
    Option 6: Domain Name Server = 192.168.243.1
    Option 5: Name Server = 24.29.103.10
    Option 15: Domain Name = "nyc.rr.com"
    Option 31: Perform Router Discover = Enabled
    End Option
```

11. In my experiment, the host requests the offered IP address in the DHCP Request message.

```
Frame 3 (350 bytes on wire, 350 bytes captured)
Ethernet II, Src: 192.168.243.92 (00:90:4b:69:dd:34), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
Internet Protocol, Src: 0.0.0.0 (0.0.0.0), Dst: 255.255.255.255 (255.255.255.255)
User Datagram Protocol, Src Port: bootpc (68), Dst Port: bootps (67)
Bootstrap Protocol
    Message type: Boot Request (1)
    Hardware type: Ethernet
    Hardware address length: 6
    Hops: 0
    Transaction ID: 0xe6746a7d
    Seconds elapsed: 1280
    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: 192.168.243.92 (00:90:4b:69:dd:34)
    Server host name not given
    Boot file name not given
    Magic cookie: (OK)
    Option 53: DHCP Message Type = DHCP Request
    Option 61: Client identifier
    Option 50: Requested IP Address = 192.168.243.92
    Option 54: Server Identifier = 192.168.243.1
    Option 12: Host Name = "homelt"
    Option 81: FQDN
    Option 60: Vendor class identifier = "MSFT 5.0"
    Option 55: Parameter Request List
    End Option
```

12. 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 3 days.

```
Frame 4 (590 bytes on wire, 590 bytes captured)
Ethernet II, Src: 192.168.243.1 (00:08:da:50:49:c5), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
Internet Protocol, Src: 192.168.243.1 (192.168.243.1), Dst: 255.255.255.255 (255.255.255.255)
User Datagram Protocol, Src Port: bootps (67), Dst Port: bootpc (68)
Bootstrap Protocol
    Message type: Boot Reply (2)
    Hardware type: Ethernet
    Hardware address length: 6
    Hops: 0
    Transaction ID: 0xe6746a7d
    Seconds elapsed: 1280
    Bootp flags: 0x0000 (Unicast)
    Client IP address: 0.0.0.0 (0.0.0.0)
    Your (client) IP address: 192.168.243.92 (192.168.243.92)
    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: 192.168.243.92 (00:90:4b:69:dd:34)
    Server host name not given
    Boot file name not given
    Magic cookie: (OK)
    Option 53: DHCP Message Type = DHCP ACK
    Option 54: Server Identifier = 192.168.243.1
    Option 51: IP Address Lease Time = 3 days
    Option 1: Subnet Mask = 255.255.255.0
    Option 3: Router = 192.168.243.1
    Option 6: Domain Name Server = 192.168.243.1
    Option 5: Name Server = 24.29.103.10
    Option 15: Domain Name = "nyc.rr.com"
    Option 31: Perform Router Discover = Enabled
    End Option
```

13. 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. 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.

```
Frame 2 (60 bytes on wire, 60 bytes captured)
Ethernet II, Src: 192.168.243.1 (00:08:da:50:49:c5), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
Address Resolution Protocol (request)
    Hardware type: Ethernet (0x0001)
    Protocol type: IP (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: request (0x0001)
    Sender MAC address: 192.168.243.1 (00:08:da:50:49:c5)
    Sender IP address: 192.168.243.1 (192.168.243.1)
    Target MAC address: 00:00:00_00:00:00 (00:00:00:00:00:00)
    Target IP address: 192.168.243.92 (192.168.243.92)
```