CS 6740, Network Security Problem Set 1 Solution

Name: Bhavik Gandhi

Email: bhavik@ccs.neu.edu

---

1. Internetworking

Describe in detail all the steps that your internet browser goes through when you click on a web page such as http://www.northeastern.edu/. You should describe which protocols are invoked (e.g., TCP, ARP, DNS, ethernet), their parameters (e.g., port numbers, addresses), network entities (e.g., DNS server, default gateway/router) and the network stack structure.

Provide screen dumps (or packets listing) from a packet sniffer such as wireshark to confirm your description.

Hints: clear your machines arp tables before clicking on the web page link, use information from ipconfig/ifconfig, route, etc.

Soln.

> Clearing ARP Table, so that the MAC address entry of getway is erased and now it only has entry for it's own IP address and Getway IP address

```
C:\Users\Bhavik>netsh interface ip delete arpcache
Ok.


C:\Users\Bhavik>arp -a
No ARP Entries Found.
```

```
C:\Users\Bhavik>ipconfig

Windows IP Configuration

Ethernet adapter Local Area Connection:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Wireless LAN adapter Wireless Network Connection:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::b82d:fe0c:d50a:e136%13
   IPv4 Address. . . . . . . . . . . : 192.168.1.22
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.1.1
```

> Now PC sends ARP broadcast packets asking who is this IP to get the MAC address of the Getway router

	Source	Destination	Protocol	Info
52	7.44738800 IntelCor_77:87:65	Broadcast	ARP	42 Who has 192.168.1.1? Tell 192.168.1.22
53	7.45010100 Netgear_cb:8c:d2	IntelCor_77:87:65	ARP	42 192.168.1.1 is at 84:1b:5e:cb:8c:d2
96	11.6593830 IntelCor_77:87:65	Broadcast	ARP	42 Who has 192.168.1.1? Tell 192.168.1.22
97	11.6615860 Netgear_cb:8c:d2	IntelCor_77:87:65	ARP	42 192.168.1.1 is at 84:1b:5e:cb:8c:d2
107	16.2448500 IntelCor_77:87:65	Broadcast	ARP	42 Who has 192.168.1.1? Tell 192.168.1.22
108	16.2500590 Netgear_cb:8c:d2	IntelCor_77:87:65	ARP	42 192.168.1.1 is at 84:1b:5e:cb:8c:d2
119	20.7545660 QuantaCo_9c:0d:dc	Broadcast	ARP	60 Who has 192.168.1.1? Tell 192.168.1.2

> In the following figure you can see the ARP broadcast request to get the MAC address of IP: 192.168.1.1

ARP Request Packet:

```
Ethernet II, Src: IntelCor_77:87:65 (68:5d:43:77:87:65), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
  Destination: Broadcast (ff:ff:ff:ff:ff:ff)
     Address: Broadcast (ff:ff:ff:ff:ff:ff)
     .... ..1. .... .... .... .... = LG bit: Locally administered address (this is NOT the factory default)
     .... ...1 .... .... .... .... = IG bit: Group address (multicast/broadcast)
  Source: IntelCor_77:87:65 (68:5d:43:77:87:65)
     Address: IntelCor_77:87:65 (68:5d:43:77:87:65)
     .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
     .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
  Type: ARP (0x0806)
Address Resolution Protocol (request)
  Hardware type: Ethernet (1)
  Protocol type: IP (0x0800)
  Hardware size: 6
  Protocol size: 4
  Opcode: request (1)
  Sender MAC address: IntelCor_77:87:65 (68:5d:43:77:87:65)
  Sender IP address: 192.168.1.22 (192.168.1.22)
  Target MAC address: 00:00:00_00:00:00 (00:00:00:00:00:00)
  Target IP address: 192.168.1.1 (192.168.1.1)
```

> Next, the PC receives the reply from IP: 192.168.1.1 with it's MAC address: 84:1b:5e:cb:8c:d2

> ARP is operated on Link Layer

ARP Reply Packet:

	Source	Destination	Protocol	Info
40	12.1558840 Netgear_cb:8c:d2	IntelCor_77:87:65	ARP	42 192.168.1.1 is at 84:1b:5e:cb:8c:d2

```
Ethernet II, Src: Netgear_cb:8c:d2 (84:1b:5e:cb:8c:d2), Dst: IntelCor_77:87:65 (68:5d:43:77:87:65)
  Destination: IntelCor_77:87:65 (68:5d:43:77:87:65)
     Address: IntelCor_77:87:65 (68:5d:43:77:87:65)
     .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
     .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
  Source: Netgear_cb:8c:d2 (84:1b:5e:cb:8c:d2)
     Address: Netgear_cb:8c:d2 (84:1b:5e:cb:8c:d2)
     .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
     .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
  Type: ARP (0x0806)
Address Resolution Protocol (reply)
  Hardware type: Ethernet (1)
  Protocol type: IP (0x0800)
  Hardware size: 6
  Protocol size: 4
  Opcode: reply (2)
  Sender MAC address: Netgear_cb:8c:d2 (84:1b:5e:cb:8c:d2)
  Sender IP address: 192.168.1.1 (192.168.1.1)
  Target MAC address: IntelCor_77:87:65 (68:5d:43:77:87:65)
  Target IP address: 192.168.1.22 (192.168.1.22)
```

> Next, open a browser and type www.neu.edu

At this point, we don't have the IP address of www.neu.edu, so it is resolved by issuing DNS request to the Getway requesting the IP address of www.neu.edu. The follwinf screenshot shows the DNS Query and Response to resolve the IP address of www.neu.edu

	Source	Destination	Protocol	Info
268	9.96980900 192.168.1.22	192.168.1.1	DNS	71 Standard query 0xf865 A www.neu.edu
269	9.99556900 192.168.1.1	192.168.1.22	DNS	218 Standard query response 0xf865 A 155.33.17.68

> DNS Queries and response are done using UDP on port 53 as can be seen in the screenshot.

```
⊞ Header checksum: 0xa857 [correct]
  Source: 192.168.1.22 (192.168.1.22)
  Destination: 192.168.1.1 (192.168.1.1)
  [Source GeoIP: Unknown]
  [Destination GeoIP: Unknown]
⊟ User Datagram Protocol, Src Port: 53735 (53735), Dst Port: domain (53)
  Source port: 53735 (53735)
  Destination port: domain (53)
  Length: 37
⊞ Checksum: 0x630c [validation disabled]
⊟ Domain Name System (query)
  [Response In: 269]
  Transaction ID: 0xf865
⊟ Flags: 0x0100 Standard query
    0... .... .... .... = Response: Message is a query
    .000 0... .... .... = Opcode: Standard query (0)
    .... ..0. .... .... = Truncated: Message is not truncated
    .... ...1 .... .... = Recursion desired: Do query recursively
    .... .... .0.. .... = Z: reserved (0)
    .... .... ...0 .... = Non-authenticated data: Unacceptable
  Questions: 1
  Answer RRs: 0
  Authority RRs: 0
  Additional RRs: 0
⊟ Queries
  ⊟ www.neu.edu: type A, class IN
      Name: www.neu.edu
      Type: A (Host address)
      Class: IN (0x0001)
```

> Next, we get the resolved IP address of www.neu.edu as DNS Response. Here we get the IP address of www.neu.edu as 155.33.17.68 as can be seen in following screenshot.

```
⊞ Header checksum: 0xb6b9 [correct]
  Source: 192.168.1.1 (192.168.1.1)
  Destination: 192.168.1.22 (192.168.1.22)
  [Source GeoIP: Unknown]
  [Destination GeoIP: Unknown]
⊟ User Datagram Protocol, Src Port: domain (53), Dst Port: 53735 (53735)
  Source port: domain (53)
  Destination port: 53735 (53735)
  Length: 184
⊞ Checksum: 0x0ed3 [validation disabled]
⊟ Domain Name System (response)
  [Request In: 268]
  [Time: 0.025760000 seconds]
  Transaction ID: 0xf865
⊞ Flags: 0x8180 Standard query response, No error
  Questions: 1
  Answer RRs: 1
  Authority RRs: 4
  Additional RRs: 2
⊟ Queries
  ⊟ www.neu.edu: type A, class IN
      Name: www.neu.edu
      Type: A (Host address)
      Class: IN (0x0001)
⊟ Answers
  ⊟ www.neu.edu: type A, class IN, addr 155.33.17.68
      Name: www.neu.edu
      Type: A (Host address)
      Class: IN (0x0001)
      Time to live: 10 minutes
      Data length: 4
      Addr: 155.33.17.68 (155.33.17.68)
```

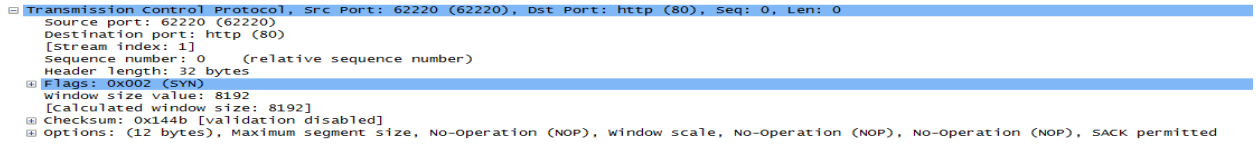
> Next, the browser picks this IP Address of www.neu.edu website and tries to establish TCP connection using 3-way handshaking (SYN, SYN-ACK, ACK)

> The following Screenshots shows the 3-way handshaking between IP Address: 192.168.1.22 (local) and 155.33.17.22(remote)

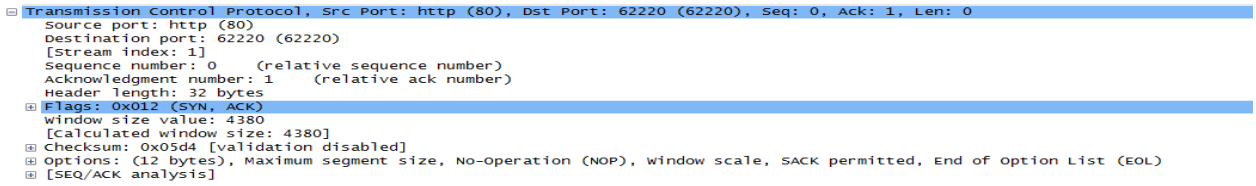
	Source	Destination	Protocol	Info
17	11.0203460 192.168.1.22	155.33.17.68	TCP	66 62220 > http [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
18	11.0954890 155.33.17.68	192.168.1.22	TCP	66 http > 62220 [SYN, ACK] Seq=0 Ack=1 Win=4380 Len=0 MSS=1460 WS=1 SACK_PERM=1
19	11.0956000 192.168.1.22	155.33.17.68	TCP	54 62220 > http [ACK] Seq=1 Ack=1 Win=17520 Len=0

> As seen,SYN, SYN-ACK, ACK is done on local port: 62220 with remote port: 80 using Http

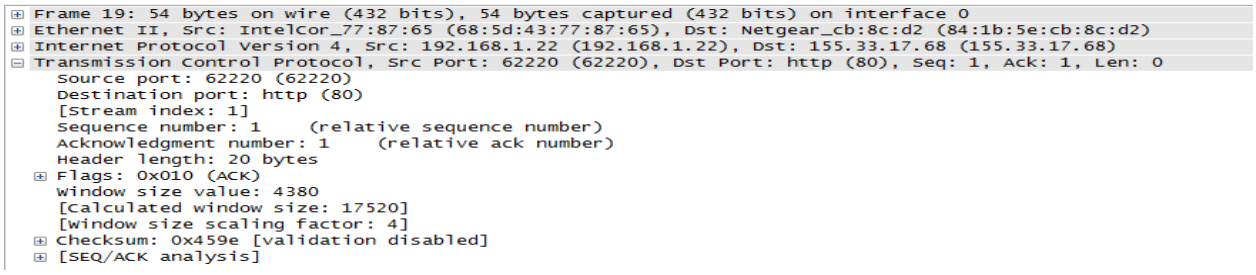
TCP SYN Packet (From local(port: 62220) to remote(port: 80))



TCP SYN-ACK Packet (From remote(port:80) to local(port:62220))

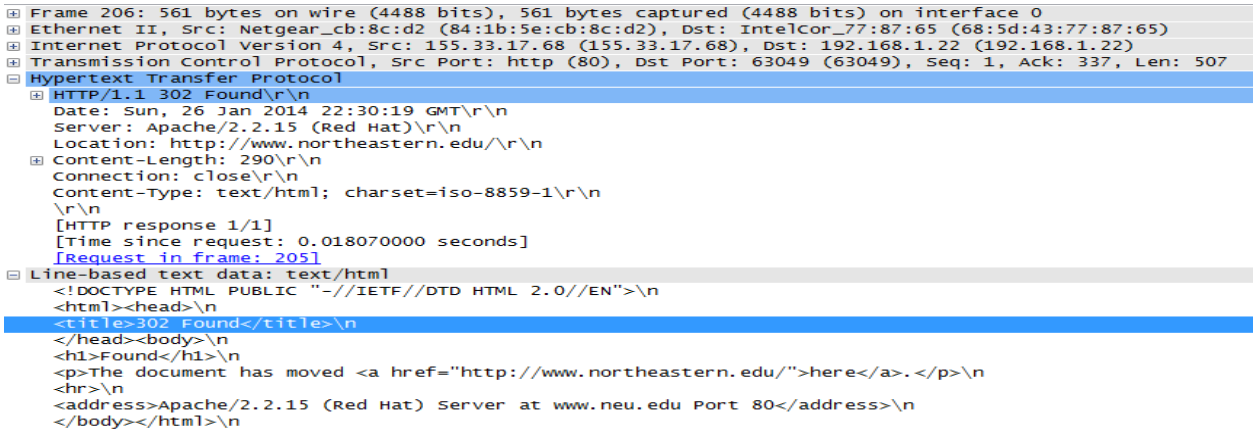


TCP ACK Packet (From local(port: 62220) to remote(port: 80)))



> Once the TCP connection is established, the browser sends the HTTP GET request to server (155.33.17.68) to get the contents of page.

> If the page is found, browser receives 302 Page found HTTP response code from server, implying the page is moved to another location specified in the response. The following screenshot shows the HTTP 302 Page Found response



> Now Browser goes to new address and fetches the contents and then displays the contents of the web page. It parses the contents of the page for HTML tags and displays the webpage on browser window.

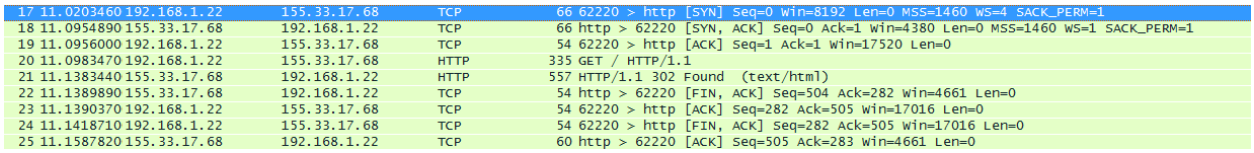
> TCP connection termination:

Once the page is loaded and server has transferred all the data to browser, server initializes TCP Session termination by sending FIN Packet, then browser Acknowledges it by sending ACK

Then Browser sends FIN packet to server saying it can terminate connection to which Server acknowledges by sending ACK back

After this the TCP connection between the server and client(browser) is terminated.

The following figure shows the TCP connection termination process between client (192.168.1.22) and server (155.33.17.68)



Network Stack:

Network Layer	**Protocol and Port**
Layer 7 - Application	HTTP (TCP port 80)
Layer 6 - Presentation	Displaying contents of web page
Layer 5 - Session	Sockets
Layer 4 - Transport	TCP, UDP (For DNS requests)
Layer 3 - Network	IP
Layer 2 - Data Link	ARP (UDP port 53)
Layer 1- Physical	Bits

2. Sockets Communication

Soln.

For Solution to this problem, open Gandhi_PS1_Q2 folder and Open ReadMe.txt to see the execution instructions