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.

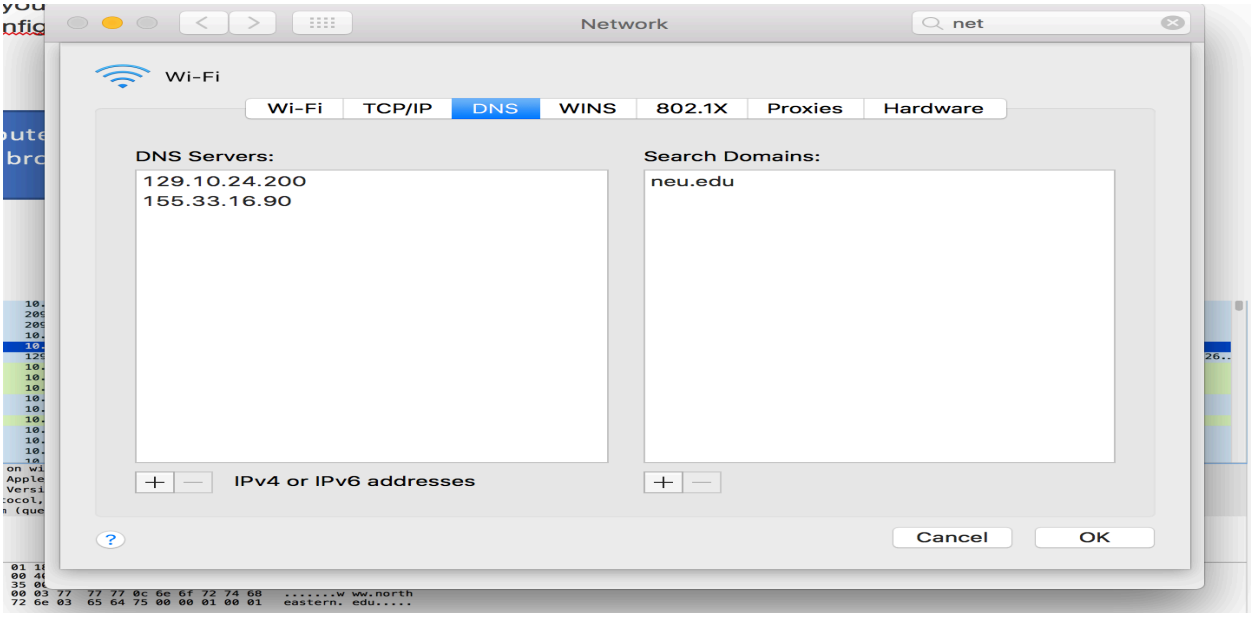
Provide screen dumps (or packets listing) from a packet sniffer such as wireshark to confirm your description.

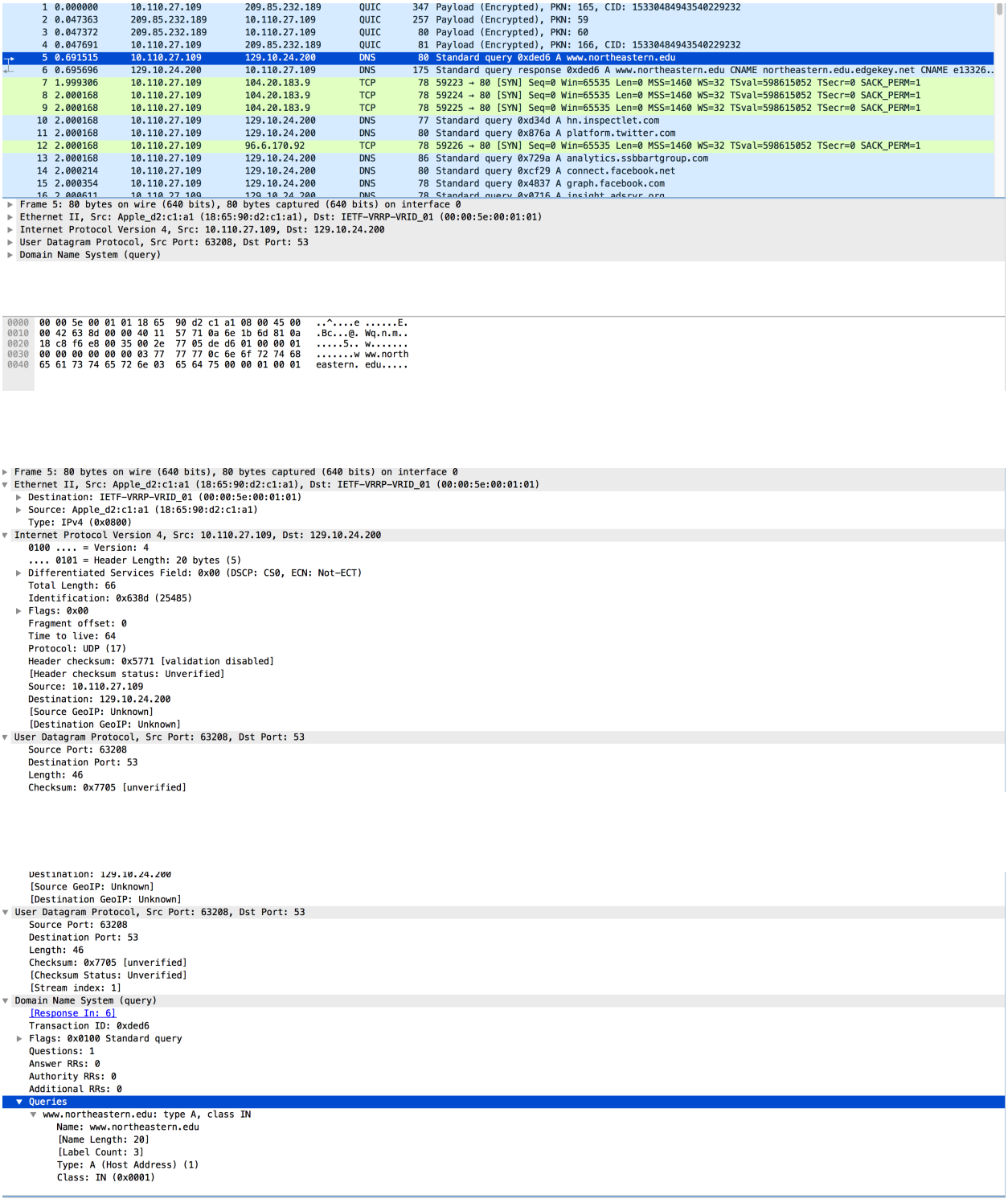
Hints: clear your machine's arp table before clicking on the web page link, use information from ipconfig/ifconfig, route, etc

Answer:
Long before the webpage is called for, the host broadcasts (ARP) Address Resolution Protocol request packets with sender IP address(an all-zero IP address). This is also referred to as broadcasting gratuitous ARP messages for updating other host's mapping of the physical hardware addresses when the sender's IP address has changed.
ARP Parameters:

Hardware Type: Ethernet (1)
Protocol Type: IP (0x0800) Hardware Size – 6
Protocol Size – 4
Sender MAC address: 18:xx:90:d2:xx:xx(hiding the mac address for security)
Sender IP Address: 0.0.0.0
Target MAC address: 00:00:00:00:00:00
Target IP Address: 129.10.24.200

DNS Query: web browser uses HTTP protocol to communicate with the web server. HTTP is application layer protocol.
The browser gets the IP Address of the URL using a process called Domain name resolution through nameservers. DNS is also an Application layer protocol. Below is a screenshot of the DNS resolution on my machine. A standard DNS query is used by the browser to request the ip address.
DNS query Parameters:
Source Port – 63349
Dest Port – Domain (53)
Source IP – 10.110.27.109





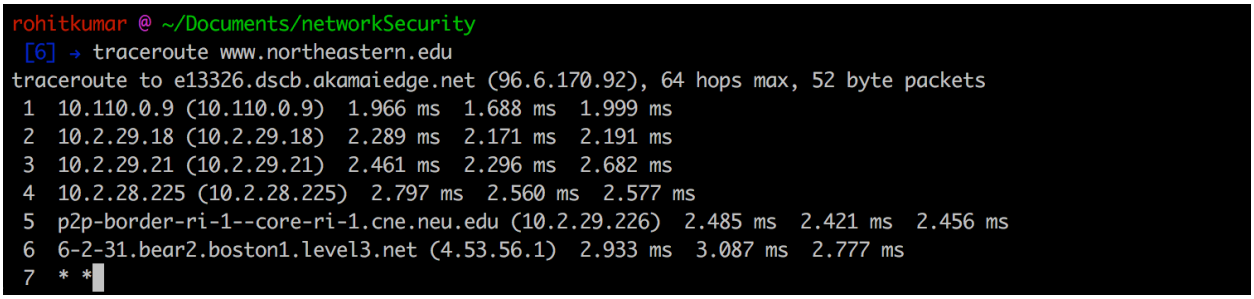
```
    1 0.000000      10.110.27.109       209.85.232.189      QUIC      347 Payload (Encrypted), PKN: 165, CID: 15330484943540229232
    2 0.047363      209.85.232.189      10.110.27.109       QUIC      257 Payload (Encrypted), PKN: 59
    3 0.047372      209.85.232.189      10.110.27.109       QUIC       80 Payload (Encrypted), PKN: 60
    4 0.047691      10.110.27.109       209.85.232.189      QUIC       81 Payload (Encrypted), PKN: 166, CID: 15330484943540229232
    5 0.691515      10.110.27.109       129.10.24.200       DNS        80 Standard query 0xded6 A www.northeastern.edu
    6 0.695696      129.10.24.200       10.110.27.109       DNS       175 Standard query response 0xded6 A www.northeastern.edu CNAME northeastern.edu.edgekey.net CNAME e13326..
    7 1.999306      10.110.27.109       104.20.183.9        TCP        78 59223 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=32 TSval=598615052 TSecr=0 SACK_PERM=1
    8 2.000168      10.110.27.109       104.20.183.9        TCP        78 59224 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=32 TSval=598615052 TSecr=0 SACK_PERM=1
    9 2.000168      10.110.27.109       104.20.183.9        TCP        78 59225 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=32 TSval=598615052 TSecr=0 SACK_PERM=1
   10 2.000168      10.110.27.109       129.10.24.200       DNS        77 Standard query 0xd34d A hn.inspectlet.com
   11 2.000168      10.110.27.109       129.10.24.200       DNS        80 Standard query 0x876a A platform.twitter.com
   12 2.000168      10.110.27.109       96.6.170.92         TCP        78 59226 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=32 TSval=598615052 TSecr=0 SACK_PERM=1
   13 2.000168      10.110.27.109       129.10.24.200       DNS        86 Standard query 0x729a A analytics.ssbbartgroup.com
   14 2.000214      10.110.27.109       129.10.24.200       DNS        80 Standard query 0xcf29 A connect.facebook.net
   15 2.000354      10.110.27.109       129.10.24.200       DNS        78 Standard query 0x4837 A graph.facebook.com
   16 2.000611      10.110.27.109       129.10.24.200       DNS        78 Standard query 0x0716 A insight.adsrvr.org
▶ Frame 5: 80 bytes on wire (640 bits), 80 bytes captured (640 bits) on interface 0
▶ Ethernet II, Src: Apple_d2:c1:a1 (18:65:90:d2:c1:a1), Dst: IETF-VRRP-VRID_01 (00:00:5e:00:01:01)
▶ Internet Protocol Version 4, Src: 10.110.27.109, Dst: 129.10.24.200
▶ User Datagram Protocol, Src Port: 63208, Dst Port: 53
▶ Domain Name System (query)

0000  00 00 5e 00 01 01 18 65  90 d2 c1 a1 08 00 45 00   ..^....e ......E.
0010  00 42 63 8d 00 00 40 11  57 71 0a 6e 1b 6d 81 0a   .Bc...@. Wq.n.m..
0020  18 c8 f6 e8 00 35 00 2e  77 05 de d6 01 00 00 01   .....5.. w.......
0030  00 00 00 00 00 00 03 77  77 77 0c 6e 6f 72 74 68   .......w ww.north
0040  65 61 73 74 65 72 6e 03  65 64 75 00 00 01 00 01   eastern. edu.....

▶ Frame 5: 80 bytes on wire (640 bits), 80 bytes captured (640 bits) on interface 0
▼ Ethernet II, Src: Apple_d2:c1:a1 (18:65:90:d2:c1:a1), Dst: IETF-VRRP-VRID_01 (00:00:5e:00:01:01)
  ▶ Destination: IETF-VRRP-VRID_01 (00:00:5e:00:01:01)
  ▶ Source: Apple_d2:c1:a1 (18:65:90:d2:c1:a1)
    Type: IPv4 (0x0800)
▼ Internet Protocol Version 4, Src: 10.110.27.109, Dst: 129.10.24.200
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  ▶ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 66
    Identification: 0x638d (25485)
  ▶ Flags: 0x00
    Fragment offset: 0
    Time to live: 64
    Protocol: UDP (17)
    Header checksum: 0x5771 [validation disabled]
    [Header checksum status: Unverified]
    Source: 10.110.27.109
    Destination: 129.10.24.200
    [Source GeoIP: Unknown]
    [Destination GeoIP: Unknown]
▼ User Datagram Protocol, Src Port: 63208, Dst Port: 53
    Source Port: 63208
    Destination Port: 53
    Length: 46
    Checksum: 0x7705 [unverified]

    Destination: 129.10.24.200
    [Source GeoIP: Unknown]
    [Destination GeoIP: Unknown]
▼ User Datagram Protocol, Src Port: 63208, Dst Port: 53
    Source Port: 63208
    Destination Port: 53
    Length: 46
    Checksum: 0x7705 [unverified]
    [Checksum Status: Unverified]
    [Stream index: 1]
▼ Domain Name System (query)
    [Response In: 6]
    Transaction ID: 0xded6
  ▶ Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  ▼ Queries
    ▼ www.northeastern.edu: type A, class IN
        Name: www.northeastern.edu
        [Name Length: 20]
        [Label Count: 3]
        Type: A (Host Address) (1)
        Class: IN (0x0001)
```

Traceroute for the call to www.northeastern.edu
This shows that a call to www.northeastern.edu went through 6 hops before resolving to a server address serving for www.northeastern.edu.



This shows that a call to www.northeastern.edu went through 6 hops before resolving to a server address serving for www.northeastern.edu.

3. Browser now creates an HTTP packet for the request. The HTTP packet is then passed to the TCP(Transmission control protocol) which is a Transport layer protocol. The main job of the TCP protocol is to establish a session in northeastern.neu.edu's server. Basically creates a secure communication pipe between the client TCP port and server's TCP port. The TCP protocol creates a packet and sends the packet to the IP layer(Internet protocol layer) which is an Internet layer protocol