# Networking Module Quiz

Obligatory OSI Seven-layer model question. Fill in the table. (Grey is not graded)

|  |  |  |  |
| --- | --- | --- | --- |
| Layer | Name | Address Type | Description, Example, or name of hardware |
| 7 | Application |  | Web browser, email, program people use |
| 6 | Presentation |  | In app layer ASCII |
| 5 | Session |  | In app and transport |
| 4 | Transport | Port number | TCP, UDP  Reliable transport |
| 3 | Network | IP address | Router  Route across Internet, … |
| 2 | Data Link | MAC address | Switch  Hosts on same subnet, … |
| 1 | Physical |  | Cable, Hub, Network Interface Card (NIC), … |

What is a **recursive** DNS lookup (5 points)?

Your DNS server queries the DNS tree, starting from a root name server if it not in cache. Not authoritative

Wireshark displays a MAC address c8:b3:73:47:d9:c4 as Cisco\_47:d9:c4. How does it know to do that?

First 3 bytes of MAC address are assigned to companies, Organizational Unique Identifier (OUI). So c8:b3:73 must belong to Cisco.

A friend tells you their computer can’t browse the Internet. When you look at their network configuration, you see this. What is the problem?  
IP address 196.168.231.15  
Mask 255.255.255.0  
Gateway 192.168.230.1

IP address and gateway are not on same subnet.

If I ping [www.google.com](http://www.google.com), will the MAC address of Google appear in my ARP cache? Why or why not?

No. My computer sends to the default gateway, so the MAC of default gateway is in my cache. Or, the layer 2 portion of the packet, which includes the MAC address, is rewritten by each router it passes through.

What is the difference between static routing and dynamic routing?

Static sets up routing table manually, example *ip route 192.168.1.0 255.255.255.0 192.168.20.1*

Dynamic uses a routing protocol to set up route table automatically. Example protocols are RIP, OSPF, BGP

When a machine boots, or gets a new IP address, how does it check to make sure that no other computer is using its IP address?

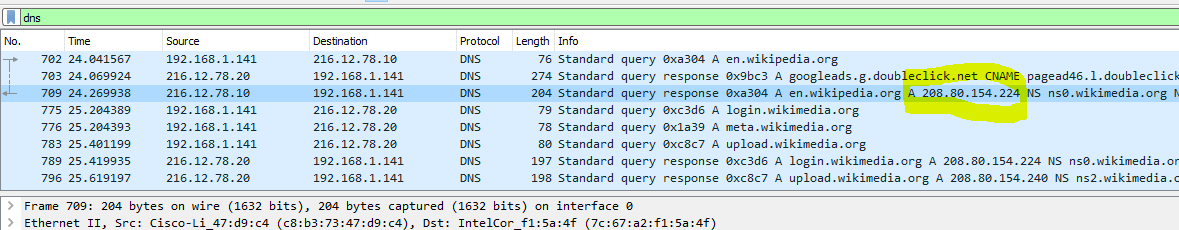
It often sends ARP broadcast requests for its own IP.

Most people never configure the IP address, mask, default gateway, and DNS server for their computer. How does the computer get that information?

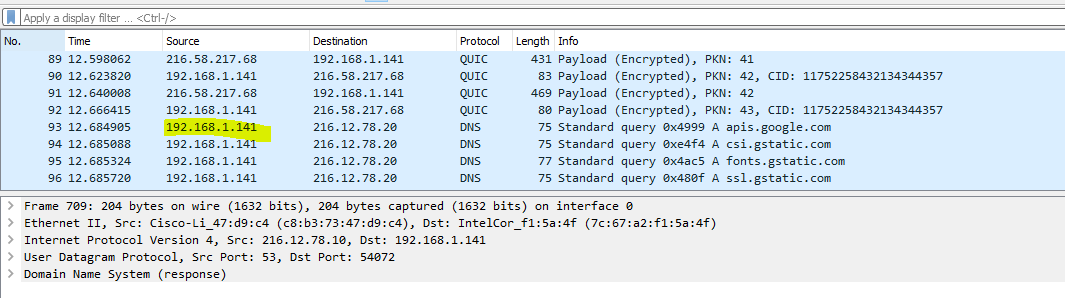
From DHCP server

Use the file NetQuiz.pcap and Wireshark to answer the following questions.

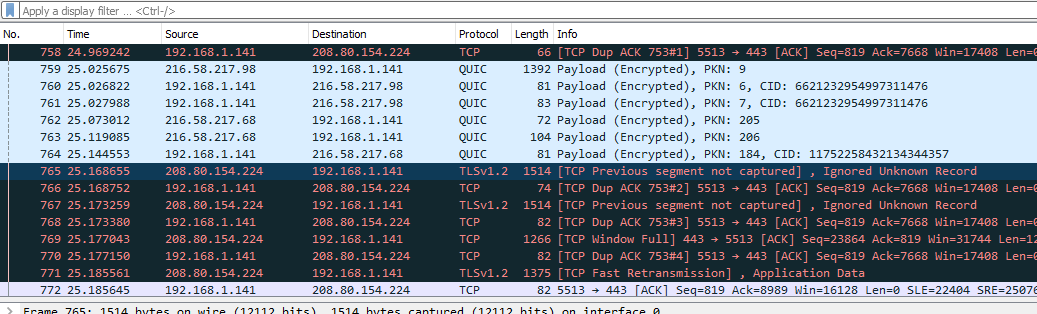
What is the IP address of en.wikipedia.org? (A display filter, dns, may help.)

208.80.154.224  


What is the IP address of the computer I used to create the pcap? It is a private address, and all the rest of the traffic is from public addresses.

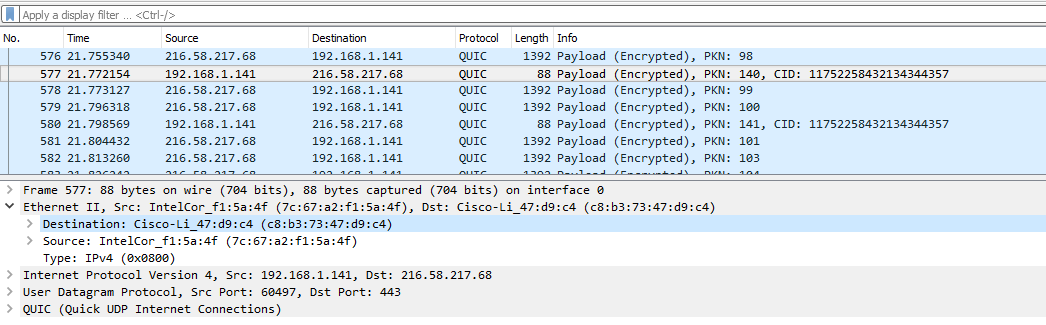
Private address ranges are 10.0.0.0/8, 172.16.0.0/12, and 192.168.0.0/16. The pcap shows a lot of traffic coming from 192.168.1.141, so that must be it.  
 

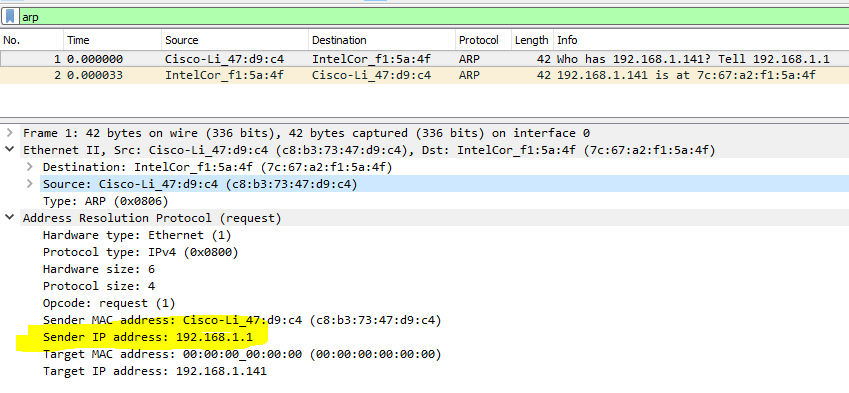
There are a lot of packets that Wireshark has marked as “TCP Dup ACK” and “TCP retransmission”. This was recorded on a (not too good) DSL connection. The page I went to, <https://en.wikipedia.org/wiki/Windows_XP>, downloaded slowly, but didn’t appear to have errors. What was going on with the “TCP Dup ACK” and “TCP retransmission” packets, and why did the page look ok?

Packets are being lost. When a packet is lost, the host resends an ACK message for the acknowledgement number it is missing (TCP Dup ACK). The host on the other end resends the packet, which Wireshark may label TCP retransmission. This way, TCP makes sure that all packets are received.  
 

What is the MAC address of my default gateway? Then, use a display filter, arp, and see if you can find the IP address of my default gateway.

All outgoing traffic from my computer (192.168.1.141) to hosts on other networks is sent to the default gateway. So, the default gateway MAC is c8:b3:73:47:d9:c4



With the display filter set to arp, we see an ARP packet with a source MAC address of c8:b3:73:47:d9:c4, and the source IP address is 192.168.1.1  


Find a three-way handshake in the packet capture. What is the frame number (left-most column, just so I know you found one) of one of the packets in the handshake?

A display filter of tcp.flags.syn makes this easier, but you don’t have to use the filter. The first handshake (SYN, SYN/ACK, ACK) in the pcap occurs in frames 13, 15 and 16, although there are many others in the pcap.