**CS 3840 Computer Networking**

**Homework 4**

Please refer to the syllabus for expectations of homework professionalism and appearance. Your homework is expected to be an individual effort. It is also expected to be neat and clearly organized. The University provides access to many software applications. Use them. Handwritten papers and poorly drawn diagrams are not acceptable. You must submit your answers of the problems in one Word or PDF file by the specified due date and time. You can find the link for your softcopy submission on Blackboard.

***Total points: 35***

The cover page of your homework will contain only the following information in the format given below:

**Name: Andrew koenig**

**700#: 700690760**

**Course #: CS 3840**

**Homework #: Homework 4**

1. [8 pts] The table below is a routing table using CIDR (Classless Inter-Domain Routing). Address bytes are denoted in binary. The notation “/23” denotes a subnet mask.

|  |  |
| --- | --- |
| Netmask/Length | Interface |
| 11000100.01011010.00000010.00000000/23 | 0 |
| 11000100.01011010.00000100.00000000/22 | 1 |
| 11000100.01011010.11000000.00000000/19 | 2 |
| 11000100.01011010.11000000.00000000/18 | 3 |
| 11000100.01011010.00000000.00000000/16 | 4 |
| 11000000.01011000.00000000.00000000/14 | 5 |
| 10000000.00000000.00000000.00000000/1 | 6 |

Select to what interface the packets with the following destination addresses will be delivered.

1. 11000100.01011010.11000011.11111100 Interface 3
2. 11000100.01011010.10101100.10001111 Interface 4
3. 11000100.01011110.00101100.10101011 Interface 5
4. 10110010.11010001.00100010.11100100 Interface 6

Wireshark Labs

1. (15 pts) Refer to <http://www-net.cs.umass.edu/wireshark-labs/Wireshark_DHCP_v8.1.doc>. Extract the file dhcp-wireshark-trace1-1 from the zip file. The display should have 1018 messages.

Filter the packets displayed in the Wireshark window by entering “dhcp” (lowercase, no quotes, and don’t forget to press return after entering!) into the display filter. Answer the following questions:

1. (1 pt) Is the DHCP Discover message sent out using UDP or TCP as the underlying transport protocol? UDP
2. (2 pts) What is the source IP address used in the IP datagram containing the Discover message? Is there anything special about this address? Explain. 0.0.0.0 This is used when the address is unspecified.
3. (2 pts) What is the destination IP address used in the datagram containing the Discover message. Is there anything special about this address? Explain. 255.255.255.255 This is a broadcast address that gets sent to every device in the network.
4. (1 pt) How do you know that the DHCP Offer message is being sent in response to the DHCP Discover message you studied in questions a-c above? The responding packet is a dhcp packet marked as offer
5. (2 pts) What is the *source* IP address used in the IP datagram containing the Offer message? Is there anything special about this address? Explain. 192.168.86.1 this is the network address, meaning it goes to the router.
6. (2 pts) What is the *destination* IP address used in the datagram containing the Offer message? Is there anything special about this address? Explain. [Hint: Look at the trace carefully. The answer to this question may differ from what you see in Figure 4.24 in the textbook. If you really want to dig into this, consult the [DHCP RFC](https://www.ietf.org/rfc/rfc2131.txt), page 24.﻿﻿﻿﻿﻿﻿﻿﻿﻿﻿﻿﻿﻿﻿﻿﻿﻿﻿﻿﻿] 192.168.86.65 This is the broadcast address meaning it will go to all devices on the network.
7. (1 pt) What is the source port number in the IP datagram containing the first DHCP Request message in your trace? What is the destination port number being used? 68, 67
8. (1 pt) What is the value in the transaction ID field of the DHCP Request message? Does it match the transaction IDs of the earlier Discover and Offer messages? 0x56f415ed, yes
9. (1 pt) What is the name of the field in the DHCP ACK message (as indicated in the Wireshark window) that contains the assigned client IP address? Client IP address
10. (1 pt) In the DHCP ACK message, for how long a time (the so-called “lease time”) has the DHPC server assigned this IP address to the client? 86400 seconds or 1 day.
11. (1 pt) What is the IP address (returned by the DHCP server to the DHCP client in the DHCP ACK message) of the first-hop router on the default path from the client to the rest of the Internet? 192.168.86.1
12. (6 pts) Refer to <http://www-net.cs.umass.edu/wireshark-labs/Wireshark_NAT_v8.1.doc>
13. . Extract the files nat-inside-wireshark-trace1-1 and nat-outside-wireshark-trace1-1 from the lab zip file.

Diagram

Description automatically generated

Answer the following questions:

In the *nat-inside-wireshark-trace1-1.pcapng* trace file, find the first HTTP GET request addressed to the external web server, as well as the subsequent HTTP response message (“200 OK”).

1. At what time does this HTTP GET message appear in the *nat-inside-wireshark-trace1-1.pcapng* trace file? 0.027362245
2. What are the source and destination IP addresses and TCP source and destination port numbers on the IP datagram carrying this HTTP GET? 192.168.10.11 138.76.29.8 port 53924 and 80
3. What are the source and destination IP addresses and source and destination ports on the IP datagram carrying the response message? 138.76.29.8 192.168.10.11 ports 80 and 53924

In the *nat-outside-wireshark-trace1-1.pcapng* trace file, find the first HTTP GET message that corresponds to the HTTP GET message that was sent from the original client to the server, as well as the subsequent HTTP response message.

1. At what time does this HTTP GET message appear in the *nat-outside-wireshark-trace1-1.pcapng* trace file? 0.027356291
2. What are the source and destination IP addresses and TCP source and destination port numbers on the IP datagram carrying this HTTP GET? 10.0.1.254 138.776.29.8 ports 56924 and 80
3. What are the source and destination IP addresses and source and destination ports on the IP datagram carrying the response message? 138.76.29.8 10.0.1.254 ports 80 and 53924i

*Notes: The time stamps in Wireshark files may be seconds since the beginning of the capture. If so, they are not synchronized. The time can be changed to other formats as follows: View menu -> Time Display Format -> select format, such as Time of Day.*

4. (6 pts) Refer to

* + 1. <http://www-net.cs.umass.edu/wireshark-labs/Wireshark_IP_v8.1.doc>
    2. .
    3. Extract the file ip-wireshark-trace2-1 from the lab zip file.

Answer the following questions:

Let’s start by taking a closer look at the 20th packet in the trace. This is a DNS AAAA request (contained in an IPv6 datagram) to an IPv6 DNS server for the IPv6 address of youtube.com.

1. What is the IPv6 source address for this datagram? Give this IPv6 address in the exact same form as displayed in the Wireshark window. 2601:193:8302:4620:215c:f5ae:8b40:a27a
2. What is the IPv6 destination address for this datagram? Give this IPv6 address in the exact same form as displayed in the Wireshark window. 2001:558:feed::1
3. What is the value of the flow label for this datagram? IN
4. How much payload data is carried in this datagram? 29 bytes

Lastly, find the IPv6 DNS response to the IPv6 DNS AAAA request made in the 20th packet in this trace.

1. How many IPv6 addresses are returned in the response to this AAAA request? 5
2. What is the first of the IPv6 addresses returned by the DNS for youtube.com? Give this IPv6 address in the exact same shorthand form as displayed in the Wireshark window. 2607:f8b0:4006:806::200e