

California State University, Monterey Bay

Week 4 – Lab 4

Group 10

Clarence Mitchell

CST311

Introduction to Computer Networks

SUMMER 2015

Instructor: Dr. Anand Seetharam

Questions and Answers

The following are the list of questions and related answers for this lab.

Wireshark 1.12.5 (v1.12.5-0-g5819e5b from master-1.12)

Filter: udp Expression... Clear Apply Save

No.	Time	Source	Destination	Protocol	Length	Info
6024	2015-05-28 22:48:00.377332000	192.168.43.87	224.0.0.252	LLMNR	74	Standard query 0x1615 A EGFD-BR-HL4070
6028	2015-05-28 22:48:00.424562000	192.168.43.60	239.255.255.250	SSDP	139	M-SEARCH * HTTP/1.1
6029	2015-05-28 22:48:00.715776000	192.168.43.87	192.168.43.255	NBNS	92	Name query NB EGFD-BR-HL4070<00>
6030	2015-05-28 22:48:01.466598000	192.168.43.87	192.168.43.255	NBNS	92	Name query NB EGFD-BR-HL4070<00>
6031	2015-05-28 22:48:03.203142000	192.168.43.87	10.32.89.30	SNMP	120	get-request 1.3.6.1.2.1.25.3.2.1.5.1 1.3.6.1.2.1.25.3.5.1.1.1 1.3.6.1.2.1.25.3.5.1.2.1
6032	2015-05-28 22:48:03.206345000	192.168.43.87	10.32.89.30	SNMP	120	get-request 1.3.6.1.2.1.25.3.2.1.5.1 1.3.6.1.2.1.25.3.5.1.1.1 1.3.6.1.2.1.25.3.5.1.2.1
6033	2015-05-28 22:48:03.206843000	192.168.43.87	10.32.89.31	SNMP	120	get-request 1.3.6.1.2.1.25.3.2.1.5.1 1.3.6.1.2.1.25.3.5.1.1.1 1.3.6.1.2.1.25.3.5.1.2.1
6034	2015-05-28 22:48:03.207301000	192.168.43.87	10.32.89.39	SNMP	120	get-request 1.3.6.1.2.1.25.3.2.1.5.1 1.3.6.1.2.1.25.3.5.1.1.1 1.3.6.1.2.1.25.3.5.1.2.1
6063	2015-05-28 22:48:03.374443000	Fe80::89Fb:e5b:647c:ff02::c		UDP	718	Source port: 55773 Destination port: 3702
6064	2015-05-28 22:48:03.389616000	192.168.43.87	239.255.255.250	UDP	698	Source port: 55772 Destination port: 3702
6065	2015-05-28 22:48:03.424696000	192.168.43.60	239.255.255.250	SSDP	139	M-SEARCH * HTTP/1.1
6066	2015-05-28 22:48:07.222022000	192.168.43.87	192.168.43.255	NBNS	92	Name query NB EGFD-BR-HL4070<00>
6067	2015-05-28 22:48:07.222500000	Fe80::89Fb:e5b:647c:ff02::1:c		LLMNR	94	Standard query 0x7ee1 A EGFD-BR-HL4070
6068	2015-05-28 22:48:07.222750000	192.168.43.87	224.0.0.252	LLMNR	74	Standard query 0x7ee1 A EGFD-BR-HL4070
6069	2015-05-28 22:48:07.222902000	Fe80::89Fb:e5b:647c:ff02::1:c		LLMNR	94	Standard query 0x0c72 AAAA EGFD-BR-HL4070
6070	2015-05-28 22:48:07.223091000	192.168.43.87	224.0.0.252	LLMNR	74	Standard query 0x0c72 AAAA EGFD-BR-HL4070
6093	2015-05-28 22:48:07.449074000	192.168.43.60	239.255.255.250	SSDP	139	M-SEARCH * HTTP/1.1

Frame 6063: 718 bytes on wire (5744 bits), 718 bytes captured (5744 bits) on interface 0

Ethernet II, Src: HonHaiPr_62:0a:cb (ac:d1:b8:62:0a:cb), Dst: IPv6mcast_0c (33:33:00:00:00:0c)

Internet Protocol version 6, Src: Fe80::89Fb:e5b:647c:f4ef (Fe80::89Fb:e5b:647c:f4ef), Dst: ff02::c (ff02::c)

User Datagram Protocol, Src Port: 55773 (55773), Dst Port: 3702 (3702)

Source Port: 55773 (55773)
 Destination Port: 3702 (3702)
 Length: 664
 Checksum: 0x8608 [validation disabled]
 [Stream index: 110]

Data (656 bytes)

- Select one UDP packet from your trace. From this packet, determine how many fields there are in the UDP header. (You shouldn't look in the textbook! Answer these questions directly from what you observe in the packet trace.) Name these fields.
 - There are four fields in the headers: source port, destination port, length, and checksum.
- By consulting the displayed information in Wireshark's packet content field for this packet, determine the length (in bytes) of each of the UDP header fields.
 - The length of each of the UDP header fields is 2 bytes long.
- The value in the Length field is the length of what? (You can consult the text for this answer). Verify your claim with your captured UDP packet.
 - The value in the length field, in the example above is 664, is the sum of the 8 header bytes and the remaining data bytes encapsulated in the packet..
- What is the maximum number of bytes that can be included in a UDP payload?(Hint: the answer to this question can be determined by your answer to 2. above)
 - The maximum number of bytes that can be in the payload is 2^{16} - the bytes already being used by the header field (8). Therefore the maximum payload is $65535-8= 65527$ bytes

5. What is the largest possible source port number? (Hint: see the hint in 4.)
 - The largest possible source port number is 2^{16} or 65535.
6. What is the protocol number for UDP? Give your answer in both hexadecimal and decimal notation. To answer this question, you'll need to look into the Protocol field of the IP datagram containing this UDP segment (see Figure 4.13 in the text, and the discussion of IP header fields).
 - The protocol number for UDP is 17 in decimal notation which in hexadecimal notation is 0x11.

6024	2015-05-28	22:48:00.377332000	192.168.43.87	224.0.0.252	LLMNR	74	Standard query 0x1615	A	EGFD-BR-HL4070
6028	2015-05-28	22:48:00.424562000	192.168.43.60	239.255.255.250	SSDP	139	M-SEARCH * HTTP/1.1		
6029	2015-05-28	22:48:00.715776000	192.168.43.87	192.168.43.255	NBNS	92	Name query NB	EGFD-BR-HL4070<00>	
6030	2015-05-28	22:48:01.466598000	192.168.43.87	192.168.43.255	NBNS	92	Name query NB	EGFD-BR-HL4070<00>	
6031	2015-05-28	22:48:03.203142000	192.168.43.87	10.32.89.30	SNMP	120	get-request	1.3.6.1.2.1.25.3.2.1.5.1 1.3.6.1.2.1.25.3.5.1.1.1 1.3.6.1.2.1.25.3.5.1.2.1	
6032	2015-05-28	22:48:03.206345000	192.168.43.87	10.32.89.30	SNMP	120	get-request	1.3.6.1.2.1.25.3.2.1.5.1 1.3.6.1.2.1.25.3.5.1.1.1 1.3.6.1.2.1.25.3.5.1.2.1	
6033	2015-05-28	22:48:03.206843000	192.168.43.87	10.32.89.31	SNMP	120	get-request	1.3.6.1.2.1.25.3.2.1.5.1 1.3.6.1.2.1.25.3.5.1.1.1 1.3.6.1.2.1.25.3.5.1.2.1	
6034	2015-05-28	22:48:03.207301000	192.168.43.87	10.32.89.39	SNMP	120	get-request	1.3.6.1.2.1.25.3.2.1.5.1 1.3.6.1.2.1.25.3.5.1.1.1 1.3.6.1.2.1.25.3.5.1.2.1	
6063	2015-05-28	22:48:03.374443000	fe80::89fb:eb5b:647c:ff02::c		UDP	17	Source port: 55773	Destination port: 3702	
6064	2015-05-28	22:48:03.389616000	192.168.43.87	239.255.255.250	UDP	698	Source port: 55772	Destination port: 3702	
6065	2015-05-28	22:48:03.424696000	192.168.43.60	239.255.255.250	SSDP	139	M-SEARCH * HTTP/1.1		
6066	2015-05-28	22:48:07.222022000	192.168.43.87	192.168.43.255	NBNS	92	Name query NB	EGFD-BR-HL4070<00>	
6067	2015-05-28	22:48:07.222500000	fe80::89fb:eb5b:647c:ff02::1:3		LLMNR	94	Standard query 0x7ee1	A	EGFD-BR-HL4070
6068	2015-05-28	22:48:07.222725000	192.168.43.87	224.0.0.252	LLMNR	74	Standard query 0x7ee1	A	EGFD-BR-HL4070
6069	2015-05-28	22:48:07.222902000	fe80::89fb:eb5b:647c:ff02::1:3		LLMNR	94	Standard query 0x0c72	AAAA	EGFD-BR-HL4070
6070	2015-05-28	22:48:07.223091000	192.168.43.87	224.0.0.252	LLMNR	74	Standard query 0x0c72	AAAA	EGFD-BR-HL4070
6093	2015-05-28	22:48:07.449074000	192.168.43.60	239.255.255.250	SSDP	139	M-SEARCH * HTTP/1.1		

Frame 6064: 698 bytes on wire (5584 bits), 698 bytes captured (5584 bits) on interface 0	
Ethernet II, Src: HonHaiPr_62:0a:cb (ac:d1:b8:62:0a:cb), Dst: IPv4mcast_7f:ff:fa (01:00:5e:7f:ff:fa)	
Internet Protocol Version 4, Src: 192.168.43.87 (192.168.43.87), Dst: 239.255.255.250 (239.255.255.250)	
Version: 4	
Header Length: 20 bytes	
Differentiated Services Field: 0xb8 (DSCP 0x2e: Expedited Forwarding; ECN: 0x00: Not-ECT (Not ECN-Capable Transport))	
Total Length: 684	
Identification: 0x2e61 (11873)	
Flags: 0x00	
Fragment offset: 0	
Time to live: 1	
Protocol: UDP (17)	
Header checksum: 0xac2e [validation disabled]	
Source: 192.168.43.87 (192.168.43.87)	
Destination: 239.255.255.250 (239.255.255.250)	
[Source GeoIP: Unknown]	
[Destination GeoIP: Unknown]	
User Datagram Protocol, Src Port: 55772 (55772), Dst Port: 3702 (3702)	
Source Port: 55772 (55772)	
Destination Port: 3702 (3702)	
Length: 664	

7. Examine a pair of UDP packets in which your host sends the first UDP packet and the second UDP packet is a reply to this first UDP packet. (Hint: for a second packet to be sent in response to a first packet, the sender of the first packet should be the destination of the second packet). Describe the relationship between the port numbers in the two packets.
 - The relationship between port numbers is that the source port on the send message is the destination port of the receive message. The destination port for the send message is also the source port for the receive message.