

CMPT 371 LAB 1

ZHAOHUI SHAN
301271015
zhaohuis@sfu.ca

❏ Select C:\Windows\system32\cmd.exe

Microsoft Windows [Version 10.0.15063]

(c) 2017 Microsoft Corporation. All rights reserved.

C:\Users\Andrew>cd\windows\system32

C:\Windows\System32>ipconfig/release

Windows IP Configuration

No operation can be performed on Local Area Connection* 10 while it has its media disconnected.

No operation can be performed on Bluetooth Network Connection while it has its media disconnected.

Wireless LAN adapter Local Area Connection* 10:

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

Wireless LAN adapter Wi-Fi:

Connection-specific DNS Suffix . :
Link-local IPv6 Address : fe80::c18:690:d63d:e427%11
Default Gateway :

Ethernet adapter Bluetooth Network Connection:

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

Tunnel adapter Teredo Tunneling Pseudo-Interface:

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

C:\Windows\System32>ipconfig/renew

Windows IP Configuration

No operation can be performed on Local Area Connection* 10 while it has its media disconnected.

No operation can be performed on Bluetooth Network Connection while it has its media disconnected.

Wireless LAN adapter Local Area Connection* 10:

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

Wireless LAN adapter Wi-Fi:

Connection-specific DNS Suffix . : tdl
Link-local IPv6 Address : fe80::c18:690:d63d:e427%11
IPv4 Address. : 10.39.149.82
Subnet Mask : 255.255.255.0
Default Gateway : 10.39.149.1

Ethernet adapter Bluetooth Network Connection:

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

Tunnel adapter Teredo Tunneling Pseudo-Interface:

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

Select C:\Windows\system32\cmd.exe

C:\Windows\System32>ipconfig/renew

Windows IP Configuration

No operation can be performed on Local Area Connection* 10 while it has its media disconnected.
No operation can be performed on Bluetooth Network Connection while it has its media disconnected.

Wireless LAN adapter Local Area Connection* 10:

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

Wireless LAN adapter Wi-Fi:

Connection-specific DNS Suffix . : tdl
Link-local IPv6 Address : fe80::c18:690:d63d:e427%11
IPv4 Address. : 10.39.149.82
Subnet Mask : 255.255.255.0
Default Gateway : 10.39.149.1

Ethernet adapter Bluetooth Network Connection:

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

Tunnel adapter Teredo Tunneling Pseudo-Interface:

Connection-specific DNS Suffix . :
IPv6 Address. : 2001:0:4137:9e76:20d7:1afe:f5d8:6aad
Link-local IPv6 Address : fe80::20d7:1afe:f5d8:6aad%30
Default Gateway : ::

C:\Windows\System32>ipconfig/release

Windows IP Configuration

No operation can be performed on Local Area Connection* 10 while it has its media disconnected.
No operation can be performed on Bluetooth Network Connection while it has its media disconnected.

Wireless LAN adapter Local Area Connection* 10:

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

Wireless LAN adapter Wi-Fi:

Connection-specific DNS Suffix . :
Link-local IPv6 Address : fe80::c18:690:d63d:e427%11
Default Gateway :

Ethernet adapter Bluetooth Network Connection:

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

Tunnel adapter Teredo Tunneling Pseudo-Interface:

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

C:\Windows\System32>ipconfig/renew

Q1.

*Wi-Fi [Wireshark 2.2.7 (v2.2.7-0-g1861a96)]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: bootp Expression... Clear Apply Save

No.	Time	Source	Destination	Protocol	Length	Info
30	14.165056	0.0.0.0	255.255.255.255	DHCP	343	DHCP Discover - Transaction ID 0xbd2caebc
31	15.364113	10.39.149.1	10.39.149.82	DHCP	342	DHCP Offer - Transaction ID 0xbd2caebc
32	15.364824	0.0.0.0	255.255.255.255	DHCP	369	DHCP Request - Transaction ID 0xbd2caebc
33	15.462237	10.39.149.1	10.39.149.82	DHCP	342	DHCP ACK - Transaction ID 0xbd2caebc
232	26.381351	10.39.149.82	172.30.129.9	DHCP	357	DHCP Request - Transaction ID 0x8a93d2e0
233	26.482176	172.30.129.9	10.39.149.82	DHCP	342	DHCP ACK - Transaction ID 0x8a93d2e0
275	44.239885	10.39.149.82	172.30.129.9	DHCP	342	DHCP Release - Transaction ID 0x667c4fff
361	63.075546	0.0.0.0	255.255.255.255	DHCP	343	DHCP Discover - Transaction ID 0xdab65638
362	63.178935	10.39.149.1	10.39.149.82	DHCP	342	DHCP Offer - Transaction ID 0xdab65638
363	63.179661	0.0.0.0	255.255.255.255	DHCP	369	DHCP Request - Transaction ID 0xdab65638
364	63.282591	10.39.149.1	10.39.149.82	DHCP	342	DHCP ACK - Transaction ID 0xdab65638

Frame 30: 343 bytes on wire (2744 bits), 343 bytes captured (2744 bits) on interface 0

Ethernet II, Src: Apple_c1:f1:b2 (3c:15:c2:c1:f1:b2), Dst: Broadcast (ff:ff:ff:ff:ff:ff)

Internet Protocol Version 4, Src: 0.0.0.0, Dst: 255.255.255.255

User Datagram Protocol, Src Port: 68, Dst Port: 67

Source Port: 68
Destination Port: 67
Length: 309
Checksum: 0xd203 [unverified]
[Checksum Status: Unverified]
[Stream index: 3]

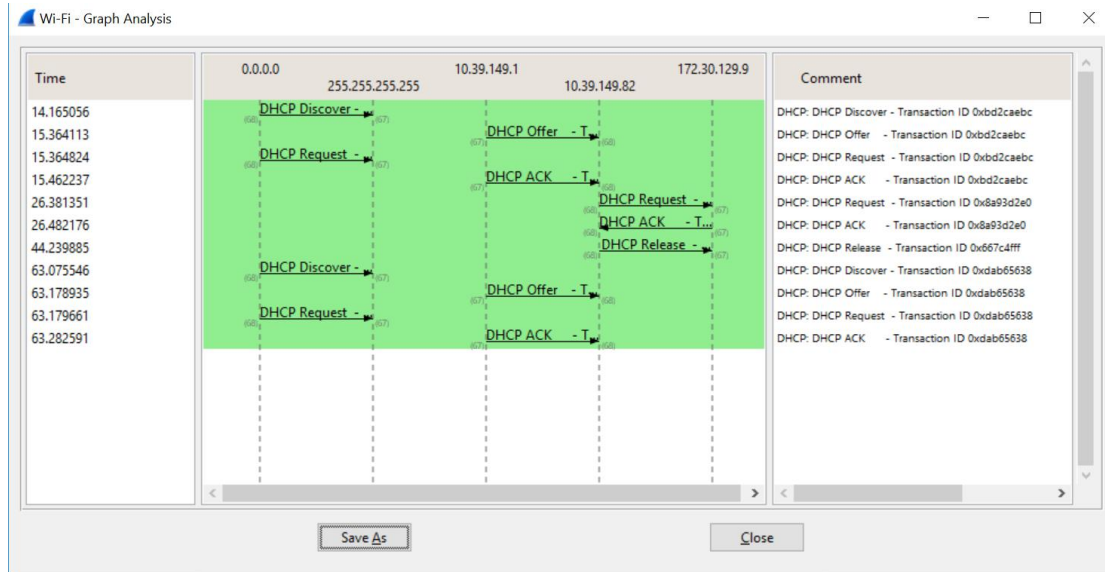
Bootstrap Protocol (Discover)

0000 ff ff ff ff ff ff 3c 15 c2 c1 f1 b2 08 00 45 00<.....E.
0010 01 49 40 1c 00 00 80 11 f9 88 00 00 00 00 ff ff ..I@.....
0020 ff ff 00 44 00 00 43 01 35 d2 03 01 01 06 00 bd 2c ...D.C.5.....
0030 ae bc 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0040 00 00 00 00 00 00 3c 15 c2 c1 f1 b2 00 00 00 00<.....
0050 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00<.....

Frame (frame), 343 bytes Packets: 553 · Displayed: 11 (2.0%) · Dropped: 0 (0.0%) Profile: Default

As the screen shot shown, the DHCP messages sent over User Datagram Protocol(UDP).

Q2.



Lab1.pcapng (Wireshark 2.2.7 (62.2.7-0-g1861a96))

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: bootp

No.	Time	Source	Destination	Protocol	Length	Info
30	14.165056	0.0.0.0	255.255.255.255	DHCP	343	DHCP Discover - Transaction ID 0xbd2caebc
31	15.364113	10.39.149.1	10.39.149.82	DHCP	342	DHCP Offer - Transaction ID 0xbd2caebc
32	15.364824	0.0.0.0	255.255.255.255	DHCP	369	DHCP Request - Transaction ID 0xbd2caebc
33	15.462237	10.39.149.1	10.39.149.82	DHCP	342	DHCP ACK - Transaction ID 0xbd2caebc
232	26.381351	10.39.149.82	172.30.129.9	DHCP	357	DHCP Request - Transaction ID 0x8a93d2e0
233	26.482176	172.30.129.9	10.39.149.82	DHCP	342	DHCP ACK - Transaction ID 0x8a93d2e0
275	44.239885	10.39.149.82	172.30.129.9	DHCP	342	DHCP Release - Transaction ID 0x667c4fff
363	63.075546	0.0.0.0	255.255.255.255	DHCP	343	DHCP Discover - Transaction ID 0xdab65638
362	63.178935	10.39.149.1	10.39.149.82	DHCP	342	DHCP Offer - Transaction ID 0xdab65638
363	63.179661	0.0.0.0	255.255.255.255	DHCP	369	DHCP Request - Transaction ID 0xdab65638
364	63.282591	10.39.149.1	10.39.149.82	DHCP	342	DHCP ACK - Transaction ID 0xdab65638

Frame 30: 343 bytes on wire (2744 bits), 343 bytes captured (2744 bits) on interface 0

Ethernet II, Src: Apple_Ci-Fi:b2 (3c:15:c2:c1:fi:b2), Dst: Broadcast (ff:ff:ff:ff:ff:ff)

Internet Protocol Version 4, Src: 0.0.0.0, Dst: 255.255.255.255

User Datagram Protocol, Src Port: 68, Dst Port: 67

Source Port: 68

Destination Port: 67

Length: 309

Checksum: 0xd203 [unverified]

[Checksum status: unverified]

[Stream Index: 3]

Bootstrap Protocol (Discover)

Lab1.pcapng (Wireshark 2.2.7 (62.2.7-0-g1861a96))

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: bootp

No.	Time	Source	Destination	Protocol	Length	Info
30	14.165056	0.0.0.0	255.255.255.255	DHCP	343	DHCP Discover - Transaction ID 0xbd2caebc
31	15.364113	10.39.149.1	10.39.149.82	DHCP	342	DHCP Offer - Transaction ID 0xbd2caebc
32	15.364824	0.0.0.0	255.255.255.255	DHCP	369	DHCP Request - Transaction ID 0xbd2caebc
33	15.462237	10.39.149.1	10.39.149.82	DHCP	342	DHCP ACK - Transaction ID 0xbd2caebc
232	26.381351	10.39.149.82	172.30.129.9	DHCP	357	DHCP Request - Transaction ID 0x8a93d2e0
233	26.482176	172.30.129.9	10.39.149.82	DHCP	342	DHCP ACK - Transaction ID 0x8a93d2e0
275	44.239885	10.39.149.82	172.30.129.9	DHCP	342	DHCP Release - Transaction ID 0x667c4fff
363	63.075546	0.0.0.0	255.255.255.255	DHCP	343	DHCP Discover - Transaction ID 0xdab65638
362	63.178935	10.39.149.1	10.39.149.82	DHCP	342	DHCP Offer - Transaction ID 0xdab65638
363	63.179661	0.0.0.0	255.255.255.255	DHCP	369	DHCP Request - Transaction ID 0xdab65638
364	63.282591	10.39.149.1	10.39.149.82	DHCP	342	DHCP ACK - Transaction ID 0xdab65638

Frame 31: 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits) on interface 0

Ethernet II, Src: Arubawet_6d:b0:c8 (00:0b:86:6d:b0:c8), Dst: Apple_Ci-Fi:b2 (3c:15:c2:c1:fi:b2)

Internet Protocol Version 4, Src: 10.39.149.1, Dst: 10.39.149.82

User Datagram Protocol, Src Port: 67, Dst Port: 68

Source Port: 67

Destination Port: 68

Length: 308

Checksum: 0xc051 [unverified]

[Checksum status: unverified]

[Stream Index: 4]

Bootstrap Protocol (Offer)

Lab1.pcapng (Wireshark 2.2.7 (62.2.7-0-g1861a96))

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: bootp

No.	Time	Source	Destination	Protocol	Length	Info
30	14.165056	0.0.0.0	255.255.255.255	DHCP	343	DHCP Discover - Transaction ID 0xbd2caebc
31	15.364113	10.39.149.1	10.39.149.82	DHCP	342	DHCP Offer - Transaction ID 0xbd2caebc
32	15.364824	0.0.0.0	255.255.255.255	DHCP	369	DHCP Request - Transaction ID 0xbd2caebc
33	15.462237	10.39.149.1	10.39.149.82	DHCP	342	DHCP ACK - Transaction ID 0xbd2caebc
232	26.381351	10.39.149.82	172.30.129.9	DHCP	357	DHCP Request - Transaction ID 0x8a93d2e0
233	26.482176	172.30.129.9	10.39.149.82	DHCP	342	DHCP ACK - Transaction ID 0x8a93d2e0
275	44.239885	10.39.149.82	172.30.129.9	DHCP	342	DHCP Release - Transaction ID 0x667c4fff
363	63.075546	0.0.0.0	255.255.255.255	DHCP	343	DHCP Discover - Transaction ID 0xdab65638
362	63.178935	10.39.149.1	10.39.149.82	DHCP	342	DHCP Offer - Transaction ID 0xdab65638
363	63.179661	0.0.0.0	255.255.255.255	DHCP	369	DHCP Request - Transaction ID 0xdab65638
364	63.282591	10.39.149.1	10.39.149.82	DHCP	342	DHCP ACK - Transaction ID 0xdab65638

Frame 32: 369 bytes on wire (2952 bits), 369 bytes captured (2952 bits) on interface 0

Ethernet II, Src: Apple_Ci-Fi:b2 (3c:15:c2:c1:fi:b2), Dst: Broadcast (ff:ff:ff:ff:ff:ff)

Internet Protocol Version 4, Src: 0.0.0.0, Dst: 255.255.255.255

User Datagram Protocol, Src Port: 68, Dst Port: 67

Source Port: 68

Destination Port: 67

Length: 335

Checksum: 0xdff3 [unverified]

[Checksum status: unverified]

[Stream Index: 3]

Bootstrap Protocol (Request)

Lab1.pcapng (Wireshark 2.2.7 (62.2.7-0-g1861a96))

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: bootp

No.	Time	Source	Destination	Protocol	Length	Info
30	14.165056	0.0.0.0	255.255.255.255	DHCP	343	DHCP Discover - Transaction ID 0xbd2caebc
31	15.364113	10.39.149.1	10.39.149.82	DHCP	342	DHCP Offer - Transaction ID 0xbd2caebc
32	15.364824	0.0.0.0	255.255.255.255	DHCP	369	DHCP Request - Transaction ID 0xbd2caebc
33	15.462237	10.39.149.1	10.39.149.82	DHCP	342	DHCP ACK - Transaction ID 0xbd2caebc
232	26.381351	10.39.149.82	172.30.129.9	DHCP	357	DHCP Request - Transaction ID 0x8a93d2e0
233	26.482176	172.30.129.9	10.39.149.82	DHCP	342	DHCP ACK - Transaction ID 0x8a93d2e0
275	44.239885	10.39.149.82	172.30.129.9	DHCP	342	DHCP Release - Transaction ID 0x667c4fff
363	63.075546	0.0.0.0	255.255.255.255	DHCP	343	DHCP Discover - Transaction ID 0xdab65638
362	63.178935	10.39.149.1	10.39.149.82	DHCP	342	DHCP Offer - Transaction ID 0xdab65638
363	63.179661	0.0.0.0	255.255.255.255	DHCP	369	DHCP Request - Transaction ID 0xdab65638
364	63.282591	10.39.149.1	10.39.149.82	DHCP	342	DHCP ACK - Transaction ID 0xdab65638

Frame 33: 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits) on interface 0

Ethernet II, Src: Arubawet_6d:b0:c8 (00:0b:86:6d:b0:c8), Dst: Apple_Ci-Fi:b2 (3c:15:c2:c1:fi:b2)

Internet Protocol Version 4, Src: 10.39.149.1, Dst: 10.39.149.82

User Datagram Protocol, Src Port: 67, Dst Port: 68

Source Port: 67

Destination Port: 68

Length: 308

Checksum: 0xbdd1 [unverified]

[Checksum status: unverified]

[Stream Index: 4]

Bootstrap Protocol (ACK)

As we can see from the screen shot Q2, the first four packet:

Discover: source port#: 68 dest port#: 67

Offer: source port#: 67 dest port#: 68

Request: source port#: 68 dest port#: 67

ACK DHCP: source port#: 67 dest port#: 68

The port numbers are same as in the example given in this lab assignment that are 67 and 68.

Q3:

Wi-Fi [Wireshark 2.2.7 (v2.2.7-0-g1861a96)]

FileEditViewGoCaptureAnalyzeStatisticsTelephonyToolsInternalsHelp

Filter: bootpExpression...ClearApplySave

No.	Time	Source	Destination	Protocol	Length	Info
30	14.165056	0.0.0.0	255.255.255.255	DHCP	343	DHCP Discover - Transaction ID 0xbd2caebc
31	15.364113	10.39.149.1	10.39.149.82	DHCP	342	DHCP Offer - Transaction ID 0xbd2caebc
32	15.364824	0.0.0.0	255.255.255.255	DHCP	369	DHCP Request - Transaction ID 0xbd2caebc
33	15.462237	10.39.149.1	10.39.149.82	DHCP	342	DHCP ACK - Transaction ID 0xbd2caebc
232	26.381351	10.39.149.82	172.30.129.9	DHCP	357	DHCP Request - Transaction ID 0x8a93d2e0
233	26.482176	172.30.129.9	10.39.149.82	DHCP	342	DHCP ACK - Transaction ID 0x8a93d2e0
275	44.239885	10.39.149.82	172.30.129.9	DHCP	342	DHCP Release - Transaction ID 0x667c4fff
361	63.075546	0.0.0.0	255.255.255.255	DHCP	343	DHCP Discover - Transaction ID 0xdab65638
362	63.178935	10.39.149.1	10.39.149.82	DHCP	342	DHCP Offer - Transaction ID 0xdab65638
363	63.179661	0.0.0.0	255.255.255.255	DHCP	369	DHCP Request - Transaction ID 0xdab65638
364	63.282591	10.39.149.1	10.39.149.82	DHCP	342	DHCP ACK - Transaction ID 0xdab65638

Frame 30: 343 bytes on wire (2744 bits), 343 bytes captured (2744 bits) on interface 0

Ethernet II, Src: Apple_c1:f1:b2 (3c:15:c2:c1:f1:b2), Dst: Broadcast (ff:ff:ff:ff:ff:ff)

Destination: Broadcast (ff:ff:ff:ff:ff:ff)

Source: Apple_c1:f1:b2 (3c:15:c2:c1:f1:b2)

Type: IPv4 (0x0800)

Internet Protocol Version 4, Src: 0.0.0.0, Dst: 255.255.255.255

User Datagram Protocol, Src Port: 68, Dst Port: 67

Source Port: 68

Destination Port: 67

Length: 309

checksum: 0xd203 [unverified]

[checksum status: unverified]

[stream index: 3]

Bootstrap Protocol (Discover)

The link-layer address: 3c:15:c2:c1:f1:b2

Q4:

Lab1.pcapng [Wireshark 2.2.7 (v2.2.7-0-g1861a96)]

FileEditViewGoCaptureAnalyzeStatisticsTelephonyToolsInternalsHelp

Filter: bootp

Expression...ClearApplySave

No.	Time	Source	Destination	Protocol	Length	Info
30	14.165056	0.0.0.0	255.255.255.255	DHCP	343	DHCP Discover - Transaction ID 0xbd2caebc
31	15.364113	10.39.149.1	10.39.149.82	DHCP	342	DHCP Offer - Transaction ID 0xbd2caebc
32	15.364824	0.0.0.0	255.255.255.255	DHCP	369	DHCP Request - Transaction ID 0xbd2caebc
33	15.462237	10.39.149.1	10.39.149.82	DHCP	342	DHCP ACK - Transaction ID 0xbd2caebc
232	26.381351	10.39.149.82	172.30.129.9	DHCP	357	DHCP Request - Transaction ID 0x8a93d2e0
233	26.482176	172.30.129.9	10.39.149.82	DHCP	342	DHCP ACK - Transaction ID 0x8a93d2e0
275	44.239885	10.39.149.82	172.30.129.9	DHCP	342	DHCP Release - Transaction ID 0x667c4fff
361	63.075546	0.0.0.0	255.255.255.255	DHCP	343	DHCP Discover - Transaction ID 0xdab65638
362	63.178935	10.39.149.1	10.39.149.82	DHCP	342	DHCP Offer - Transaction ID 0xdab65638
363	63.179661	0.0.0.0	255.255.255.255	DHCP	369	DHCP Request - Transaction ID 0xdab65638
364	63.282591	10.39.149.1	10.39.149.82	DHCP	342	DHCP ACK - Transaction ID 0xdab65638

Message type: Boot Request (1)
Hardware type: Ethernet (0x01)
Hardware address length: 6
Hops: 0
Transaction ID: 0xbd2caebc
Seconds elapsed: 0
Bootstrap flags: 0x0000 (Unicast)
Client IP address: 0.0.0.0
Your (client) IP address: 0.0.0.0
Next server IP address: 0.0.0.0
Relay agent IP address: 0.0.0.0
Client MAC address: Apple_c1:f1:b2 (3c:15:c2:c1:f1:b2)
Client hardware address padding: 0000000000000000000000
Server host name not given
Boot file name not given
Magic cookie: DHCP
Option (53) DHCP Message Type (Request)
Length: 1
DHCP: Request (3)
Option (61) Client identifier
Length: 7
Hardware type: Ethernet (0x01)
Client MAC address: Apple_c1:f1:b2 (3c:15:c2:c1:f1:b2)
Option (50) Requested IP Address
Length: 4
0110 00 00 00 00 00 00 63 82 53 63 35 01 03 3d 07 01Sg5...
0120 3c 15 c2 c1 f1 b2 32 04 0a 27 95 32 36 04 ac 1e <....2...R6...
0130 81 09 0c 0f 44 45 53 4b 54 4f 50 2d 4b 52 48 4a ...DESK TOP-KRM3
0140 55 54 36 51 12 00 00 00 44 45 53 4b 54 4f 50 2d UT6Q...DESKTOP-
0150 4b 52 48 4a 55 54 36 3c 08 4d 53 46 54 20 35 2e KRHJUT6K...MSFT 5...
0160 30 27 0a 01 02 02 0e 16 21 2b 2c 2e 2f 20 4b 4f 67
Bootp/Dhcp option type (bootp.option.type...) Packets: 553 - Displayed: 11 (2.0%) - Dropped: 0 (0.0%) Profile: Default

Lab1.pcapng [Wireshark 2.2.7 (v2.2.7-0-g1861a96)]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: bootp Expression... Clear Apply Save

No.	Time	Source	Destination	Protocol	Length	Info
30	14.165056	0.0.0.0	255.255.255.255	DHCP	343	DHCP Discover - Transaction ID 0xbd2caebc
31	15.364113	10.39.149.1	10.39.149.82	DHCP	342	DHCP Offer - Transaction ID 0xbd2caebc
32	15.364824	0.0.0.0	255.255.255.255	DHCP	369	DHCP Request - Transaction ID 0xbd2caebc
33	15.462237	10.39.149.1	10.39.149.82	DHCP	342	DHCP ACK - Transaction ID 0xbd2caebc
232	26.381351	10.39.149.82	172.30.129.9	DHCP	357	DHCP Request - Transaction ID 0x8a93d2e0
233	26.482176	172.30.129.9	10.39.149.82	DHCP	342	DHCP ACK - Transaction ID 0x8a93d2e0
275	44.239885	10.39.149.82	172.30.129.9	DHCP	342	DHCP Release - Transaction ID 0x667c4fff
361	63.075546	0.0.0.0	255.255.255.255	DHCP	343	DHCP Discover - Transaction ID 0xdab65638
362	63.178935	10.39.149.1	10.39.149.82	DHCP	342	DHCP Offer - Transaction ID 0xdab65638
363	63.179661	0.0.0.0	255.255.255.255	DHCP	369	DHCP Request - Transaction ID 0xdab65638
364	63.282591	10.39.149.1	10.39.149.82	DHCP	342	DHCP ACK - Transaction ID 0xdab65638

Hops: 0
Transaction ID: 0xbd2caebc
Seconds elapsed: 0
Bootp flags: 0x0000 (unicast)
Client IP address: 0.0.0.0
Your (client) IP address: 0.0.0.0
Next server IP address: 0.0.0.0
Relay agent IP address: 0.0.0.0
Client MAC address: Apple_c1:f1:b2 (3c:15:c2:c1:f1:b2)
Client hardware address padding: 00000000000000000000
Server host name not given
Boot file name not given
Magic cookie: DHCP

Option: (53) DHCP Message Type (Discover)
Length: 1
DHCP: Discover (1)
Option: (61) Client Identifier
Length: 7
Hardware type: Ethernet (0x01)
Client MAC address: Apple_c1:f1:b2 (3c:15:c2:c1:f1:b2)
Option: (50) Requested IP Address
Length: 4
Requested IP Address: 10.39.149.82
Option: (12) Host Name
Length: 15

0110 00 00 00 00 00 00 63 82 53 63 3c 01 01 3d 07 01C. S...
0120 3c 15 c2 c1 f1 b2 32 04 0a 27 35 55 0c 0f 44 452. R...DE
0130 53 4b 54 4f 50 2d 4b 52 48 4a 55 54 36 3c 08 4d SKTOP-KR HJUTG<M
0140 53 46 54 20 35 2a 30 37 0d 01 03 06 0f 1f 21 2b SFT 5.07!
0150 2c 2a 2f 79 f9 fc ff

Bootp/Dhcp option type (bootp.option.type...) | Packets: 553 - Displayed: 11 (2.0%) - Dropped: 0 (0.0%) | Profile: Default

The value in the DHCP discover message differentiate this message from the DHCP request message is: Option(53)

Q5:

No.	Time	Source	Destination	Protocol	Length	Info
30	14.165056	0.0.0.0	255.255.255.255	DHCP	343	DHCP Discover - Transaction ID 0xbd2caebc
31	15.364113	10.39.149.1	10.39.149.82	DHCP	342	DHCP Offer - Transaction ID 0xbd2caebc
32	15.364824	0.0.0.0	255.255.255.255	DHCP	369	DHCP Request - Transaction ID 0xbd2caebc
33	15.462237	10.39.149.1	10.39.149.82	DHCP	342	DHCP ACK - Transaction ID 0xbd2caebc

The value of the Transaction-ID in the first four DHCP messages is 0xbd2caebc

232	26.381351	10.39.149.82	172.30.129.9	DHCP	357	DHCP Request - Transaction ID 0x8a93d2e0
233	26.482176	172.30.129.9	10.39.149.82	DHCP	342	DHCP ACK - Transaction ID 0x8a93d2e0

The value of the Transaction-Id in the 2nd set of DHCP messages is 0x8a93d2e0

The purpose is that by different transaction-ID, the DHCP server can differentiate between different requests that made by users.

Q6:

No.	Time	Source	Destination	Protocol	Length	Info
30	14.165056	0.0.0.0	255.255.255.255	DHCP	343	DHCP Discover - Transaction ID 0xbd2caebc
31	15.364113	10.39.149.1	10.39.149.82	DHCP	342	DHCP Offer - Transaction ID 0xbd2caebc
32	15.364824	0.0.0.0	255.255.255.255	DHCP	369	DHCP Request - Transaction ID 0xbd2caebc
33	15.462237	10.39.149.1	10.39.149.82	DHCP	342	DHCP ACK - Transaction ID 0xbd2caebc

Discover: source IP#:0.0.0.0

dest IP#: 255.255.255.255

Offer: source IP#:10.39.149.1

dest IP#: 10.39.149.82

Request: source IP#:0.0.0.0

dest IP#: 255.255.255.255

ACK DHCP: source IP#:10.39.149.1

dest IP#: 10.39.149.82

Q7:

33	15.462237	10.39.149.1	10.39.149.82	DHCP	342	DHCP ACK	- Transaction ID 0xbd2caebc
----	-----------	-------------	--------------	------	-----	----------	-----------------------------

The IP address if DHCP server is: 10.39.149.1

Q8:

Lab1.pcapng [Wireshark 2.2.7 (v2.2.7-0-g1861a96)]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: bootp Expression... Clear Apply Save

No.	Time	Source	Destination	Protocol	Length	Info
30	14.165056	0.0.0.0	255.255.255.255	DHCP	343	DHCP Discover - Transaction ID 0xbd2caebc
31	15.364113	10.39.149.1	10.39.149.82	DHCP	342	DHCP Offer - Transaction ID 0xbd2caebc
32	15.364824	0.0.0.0	255.255.255.255	DHCP	369	DHCP Request - Transaction ID 0xbd2caebc
33	15.462237	10.39.149.1	10.39.149.82	DHCP	342	DHCP ACK - Transaction ID 0xbd2caebc
232	26.381351	10.39.149.82	172.30.129.9	DHCP	357	DHCP Request - Transaction ID 0x8a93d2e0
233	26.482176	172.30.129.9	10.39.149.82	DHCP	342	DHCP ACK - Transaction ID 0x8a93d2e0
275	44.239885	10.39.149.82	172.30.129.9	DHCP	342	DHCP Release - Transaction ID 0x667c4fff
361	63.075546	0.0.0.0	255.255.255.255	DHCP	343	DHCP Discover - Transaction ID 0xdab65638
362	63.178935	10.39.149.1	10.39.149.82	DHCP	342	DHCP Offer - Transaction ID 0xdab65638
363	63.179661	0.0.0.0	255.255.255.255	DHCP	369	DHCP Request - Transaction ID 0xdab65638
364	63.282591	10.39.149.1	10.39.149.82	DHCP	342	DHCP ACK - Transaction ID 0xdab65638

Hardware address length: 6
Hops: 1
Transaction ID: 0xbd2caebc
Seconds elapsed: 0
☒ Bootp flags: 0x0000 (Unicast)
Client IP address: 0.0.0.0
Your (client) IP address: 10.39.149.82
Next server IP address: 0.0.0.0
Relay agent IP address: 10.39.149.1
Client MAC address: Apple_c1:f1:b2 (3c:15:c2:c1:f1:b2)
Client hardware address padding: 00000000000000000000
Server host name not given
Boot file name not given
Magic cookie: DHCP
☒ Option: (53) DHCP Message Type (Offer)
Length: 1
DHCP: Offer (2)
☒ Option: (54) DHCP Server Identifier
Length: 4
DHCP Server Identifier: 172.30.129.9
☒ Option: (51) IP Address Lease Time
Length: 4
IP Address Lease Time: (1200s) 20 minutes
☒ Option: (1) Subnet Mask
Length: 4

0030 ae bc 00 00 00 00 00 00 00 00 0a 27 95 52 00 00R.
0040 00 00 0a 27 95 01 3c 15 c2 c1 f1 b2 00 00 00 00<.....
0050 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0060 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0070 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0080 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Your (client) IP address (bootp.ip.your), 4 bytes
Packets: 553 · Displayed: 11 (2.0%) · Dropped: 0 (0.0%) Profile: Default

The IP address the DHCP server offering to my host in the DHCP Offer message is: 10.39.149.82

The DHCP message with “Option: (53) DHCP Message Type (offer)” contains the offered DHCP address.

Q9:

Lab1.pcapng [Wireshark 2.2.7 (v2.2.7-0-g1861a96)]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: bootp Expression... Clear Apply Save

No.	Time	Source	Destination	Protocol	Length	Info
30	14.165056	0.0.0.0	255.255.255.255	DHCP	343	DHCP Discover - Transaction ID 0xbd2caebc
31	15.364113	10.39.149.1	10.39.149.82	DHCP	342	DHCP Offer - Transaction ID 0xbd2caebc
32	15.364824	0.0.0.0	255.255.255.255	DHCP	369	DHCP Request - Transaction ID 0xbd2caebc
33	15.462237	10.39.149.1	10.39.149.82	DHCP	342	DHCP ACK - Transaction ID 0xbd2caebc
232	26.381351	10.39.149.82	172.30.129.9	DHCP	357	DHCP Request - Transaction ID 0x8a93d2e0
233	26.482176	172.30.129.9	10.39.149.82	DHCP	342	DHCP ACK - Transaction ID 0x8a93d2e0
275	44.239885	10.39.149.82	172.30.129.9	DHCP	342	DHCP Release - Transaction ID 0x667c4fff
361	63.075546	0.0.0.0	255.255.255.255	DHCP	343	DHCP Discover - Transaction ID 0xdab65638
362	63.178935	10.39.149.1	10.39.149.82	DHCP	342	DHCP Offer - Transaction ID 0xdab65638
363	63.179661	0.0.0.0	255.255.255.255	DHCP	369	DHCP Request - Transaction ID 0xdab65638
364	63.282591	10.39.149.1	10.39.149.82	DHCP	342	DHCP ACK - Transaction ID 0xdab65638

User Datagram Protocol, Src Port: 68, Dst Port: 67

Bootstrap Protocol (Discover)

- Message type: Boot Request (1)
- Hardware type: Ethernet (0x01)
- Hardware address length: 6
- Hops: 0
- Transaction ID: 0xbd2caebc
- Seconds elapsed: 0
- Bootp flags: 0x0000 (Unicast)
- Client IP address: 0.0.0.0
- Your (client) IP address: 0.0.0.0
- Next server IP address: 0.0.0.0
- Relay agent IP address: 0.0.0.0
- Client MAC address: Apple_c1:f1:b2 (3c:15:c2:c1:f1:b2)
- Client hardware address padding: 00000000000000000000
- Server host name not given
- Boot file name not given
- Magic cookie: DHCP
- Option: (53) DHCP Message Type (Discover)
 - Length: 1
 - DHCP: Discover (1)
- Option: (61) Client identifier
 - Length: 7
 - Hardware type: Ethernet (0x01)
 - Client MAC address: Apple_c1:f1:b2 (3c:15:c2:c1:f1:b2)
- Option: (50) Requested IP Address

0000 ff ff ff ff ff ff 3c 15 c2 c1 f1 b2 08 00 45 00<.E.
0010 01 49 40 1c 00 00 80 11 f9 88 00 00 00 00 ff ff .I@....
0020 ff ff 00 44 00 00 43 01 35 d2 03 01 01 06 00 bd 2c ...D.C.5
0030 ae bc 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0040 00 00 00 00 00 00 3c 15 c2 c1 f1 b2 00 00 00 00<.
0050 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

File: "C:\Users\Andrew\Desktop\Lab1.pcapng" Packets: 553 - Displayed: 11 (2.0%) - Dropped: 0 (0.0%) Profile: Default

In the example screenshot, the value that indicates there is no relay agent is 0.0.0.0. As the screenshot of my experiment above, there is no relay agent as well.

Q10

The router line tells where the client should send messages by default
The subnet mask line tells the client which subnet mask should use

Q11

Lab1.pcapng [Wireshark 2.2.7 (v2.2.7-0-g1861a96)]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: bootp Expression... Clear Apply Save

No.	Time	Source	Destination	Protocol	Length	Info
30	14.165056	0.0.0.0	255.255.255.255	DHCP	343	DHCP Discover - Transaction ID 0xbd2cae
31	15.364113	10.39.149.1	10.39.149.82	DHCP	342	DHCP Offer - Transaction ID 0xbd2cae
32	15.364824	0.0.0.0	255.255.255.255	DHCP	369	DHCP Request - Transaction ID 0xbd2cae
33	15.462237	10.39.149.1	10.39.149.82	DHCP	342	DHCP ACK - Transaction ID 0xbd2cae
232	26.381351	10.39.149.82	172.30.129.9	DHCP	357	DHCP Request - Transaction ID 0x8a93d2e0
233	26.482176	172.30.129.9	10.39.149.82	DHCP	342	DHCP ACK - Transaction ID 0x8a93d2e0
275	44.239885	10.39.149.82	172.30.129.9	DHCP	342	DHCP Release - Transaction ID 0x667c4fff
361	63.075546	0.0.0.0	255.255.255.255	DHCP	343	DHCP Discover - Transaction ID 0xdab65638
362	63.178935	10.39.149.1	10.39.149.82	DHCP	342	DHCP Offer - Transaction ID 0xdab65638
363	63.179661	0.0.0.0	255.255.255.255	DHCP	369	DHCP Request - Transaction ID 0xdab65638
364	63.282591	10.39.149.1	10.39.149.82	DHCP	342	DHCP ACK - Transaction ID 0xdab65638

Magic Cookie: DHCP

- Option: (53) DHCP Message Type (Request)
Length: 1
DHCP: Request (3)
- Option: (61) Client identifier
Length: 7
Hardware type: Ethernet (0x01)
Client MAC address: Apple_c1:f1:b2 (3c:15:c2:c1:f1:b2)
- Option: (50) Requested IP Address
Length: 4
Requested IP Address: 10.39.149.82
- Option: (54) DHCP Server Identifier
Length: 4
DHCP Server Identifier: 172.30.129.9
- Option: (12) Host Name
Length: 15
Host Name: DESKTOP-KRHJUT6
- Option: (81) Client Fully Qualified Domain Name
Length: 18
Flags: 0x00
A-RR result: 0
PTR-RR result: 0
Client name: DESKTOP-KRHJUT6
- Option: (60) Vendor class identifier
Length: 8
Vendor class identifier: MSFT 5.0

0120 3c 15 c2 c1 f1 b2 32 04 0a 27 95 52 36 04 ac 1e <....2. .R6...
0130 81 09 0c 0f 44 45 53 4b 54 4f 50 2d 4b 52 48 4aDESK TOP-KRHJ
0140 55 54 36 51 12 00 00 00 44 45 53 4b 54 4f 50 2d UT6Q.... DESKTOP-
0150 4b 52 48 4a 55 54 36 3c 08 4d 53 46 54 20 35 2e KRHJUT6< .MSFT 5.
0160 30 37 0d 01 03 06 0f 1f 21 2b 2c 2e 2f 79 f9 fc 07..... !+./y..
0170 ff

Option 50: Requested IP Address (bootp.opti... Packets: 553 · Displayed: 11 (2.0%) · Dropped: 0 (0.0%) Profile: Default

As we can see from Question8 above, the DHCP offer IP address is: 10.39.149.82 (DHCP Offer)

By looking the screenshot above, the client accept this IP address, and we can see the "Requested IP Address: 10.39.149.82"

Lab1.pcapng [Wireshark 2.2.7 (v2.2.7-0-g1861a96)]

The lease time is the amount of time the DHCP server assigned an IP address to client. Within the lease time, the DHCP server will not assign this specific IP address to another client. After the lease time expired, this IP address can be reused by the DHCP server to give to other client.

As the screenshot above, the lease time is (1200s)=20minutes.

Q13

The DHCP release message is the message that the client sent to cancel the lease of IP address that was given by DHCP server.

There is no acknowledgment of receipt of the client's DHCP request.

If the DHCP release message is lost, the client had released the IP address. However, the DHCP server has to wait this specific IP address to be expired before the DHCP server can reassign this IP address.

Q14.

Wireshark 2.2.7 (v2.2.7-0-g1861a96) interface showing a packet capture on Wi-Fi. The filter is set to 'bootp || arp'. The packet list shows the following entries:

No.	Time	Source	Destination	Protocol	Length	Info
18	7.027887	0.0.0.0	255.255.255.255	DHCP	343	DHCP Discover - Transaction ID 0xbb40a1bf
19	7.141342	10.39.149.1	10.39.149.82	DHCP	342	DHCP Offer - Transaction ID 0xbb40a1bf
20	7.142061	0.0.0.0	255.255.255.255	DHCP	369	DHCP Request - Transaction ID 0xbb40a1bf
21	7.236213	10.39.149.1	10.39.149.82	DHCP	342	DHCP ACK - Transaction ID 0xbb40a1bf
29	7.264217	Apple_c1:f1:b2	Broadcast	ARP	42	who has 10.39.149.1? Tell 10.39.149.82
30	7.278401	Apple_c1:f1:b2	Broadcast	ARP	42	who has 10.39.149.82? Tell 0.0.0.0
33	7.297949	Apple_c1:f1:b2	Broadcast	ARP	42	who has 10.39.149.1? Tell 10.39.149.82
59	7.356227	Apple_c1:f1:b2	Broadcast	ARP	42	who has 10.39.149.1? Tell 10.39.149.82
60	7.398509	ArubaNet_6d:b0:c8	Apple_c1:f1:b2	ARP	42	10.39.149.1 is at 00:0b:86:6d:b0:c8
62	7.403003	ArubaNet_6d:b0:c8	Apple_c1:f1:b2	ARP	42	10.39.149.1 is at 00:0b:86:6d:b0:c8
64	7.471591	ArubaNet_6d:b0:c8	Apple_c1:f1:b2	ARP	42	10.39.149.1 is at 00:0b:86:6d:b0:c8
86	8.281709	Apple_c1:f1:b2	Broadcast	ARP	42	who has 10.39.149.82? Tell 0.0.0.0
110	9.285109	Apple_c1:f1:b2	Broadcast	ARP	42	who has 10.39.149.82? Tell 0.0.0.0
150	10.287576	Apple_c1:f1:b2	Broadcast	ARP	42	Gratuitous ARP for 10.39.149.82 (Request)
172	10.842601	ArubaNet_6d:b0:c8	Broadcast	ARP	56	who has 10.39.149.131? Tell 10.39.149.1
185	11.865175	ArubaNet_6d:b0:c8	Broadcast	ARP	56	who has 10.39.149.131? Tell 10.39.149.1
188	12.889296	ArubaNet_6d:b0:c8	Broadcast	ARP	56	who has 10.39.149.131? Tell 10.39.149.1
191	14.117885	ArubaNet_6d:b0:c8	Broadcast	ARP	56	who has 10.39.149.131? Tell 10.39.149.1
194	15.141839	ArubaNet_6d:b0:c8	Broadcast	ARP	56	who has 10.39.149.131? Tell 10.39.149.1
195	15.224454	10.39.149.82	172.30.129.9	DHCP	357	DHCP Request - Transaction ID 0x48cd6543
202	15.492181	172.30.129.9	10.39.149.82	DHCP	342	DHCP ACK - Transaction ID 0x48cd6543
217	15.966526	ArubaNet_6d:b0:c8	Broadcast	ARP	56	who has 10.39.149.131? Tell 10.39.149.1
226	19.349238	ArubaNet_6d:b0:c8	Broadcast	ARP	56	who has 10.39.149.131? Tell 10.39.149.1
228	20.466758	ArubaNet_6d:b0:c8	Broadcast	ARP	56	who has 10.39.149.131? Tell 10.39.149.1
231	21.388062	ArubaNet_6d:b0:c8	Broadcast	ARP	56	who has 10.39.149.131? Tell 10.39.149.1
232	24.361609	10.39.149.82	172.30.129.9	DHCP	342	DHCP Release - Transaction ID 0x5634ea89
254	26.302990	oneplusT_5a:2d:fc	Broadcast	ARP	42	who has 10.39.149.1? Tell 10.39.149.111
256	28.779684	0.0.0.0	255.255.255.255	DHCP	343	DHCP Discover - Transaction ID 0x6f544629
257	28.876705	10.39.149.1	10.39.149.82	DHCP	342	DHCP Offer - Transaction ID 0x6f544629
258	28.877416	0.0.0.0	255.255.255.255	DHCP	369	DHCP Request - Transaction ID 0x6f544629
259	28.992269	10.39.149.1	10.39.149.82	DHCP	342	DHCP ACK - Transaction ID 0x6f544629

Frame 9: 56 bytes on wire (448 bits), 56 bytes captured (448 bits) on interface 0
Ethernet II, Src: ArubaNet_6d:b0:c8 (00:0b:86:6d:b0:c8), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
Address Resolution Protocol (request)

0000 ff ff ff ff ff ff 00 0b 86 6d b0 c8 08 06 00 01m.....
0010 08 00 06 04 00 01 00 0b 86 6d b0 c8 0a 27 95 01m.....
0020 00 00 00 00 00 00 0a 27 95 83 00 00 00 00 00 00
0030 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
.....

File: "C:\Users\Andrew\AppData\Local\Temp\... Packets: 403 · Displayed: 46 (11.4%) · Dropped: 0 (0.0%) Profile: Default

There is ARP request made by the DHCP server.

Since before offer an IP address to a client, the DHCP server send an ARP request for the offered IP address to confirm that this IP address is not used by other client.