Sheridan College		
Course	Data Network Design and Configuration – Routers and Switches	
Professor	Ida Leung	
Student Name/ID	Kunjan Patel/991535676	
Table number		
Lab 1: Wireshark Practise		
Performed Date	19/5/2019	
Instructor's Sign		(marks)

OBJECTIVES:

Review the use of wireshark and how to use the captured data

Step 1: Use Wireshark to capture the following protocols in complete set (include sender and receiver both direction full conversation(:

- 1. DHCP
- 2. DNS

Step 2: Printscreen and document your capture for each data flow for the protocol

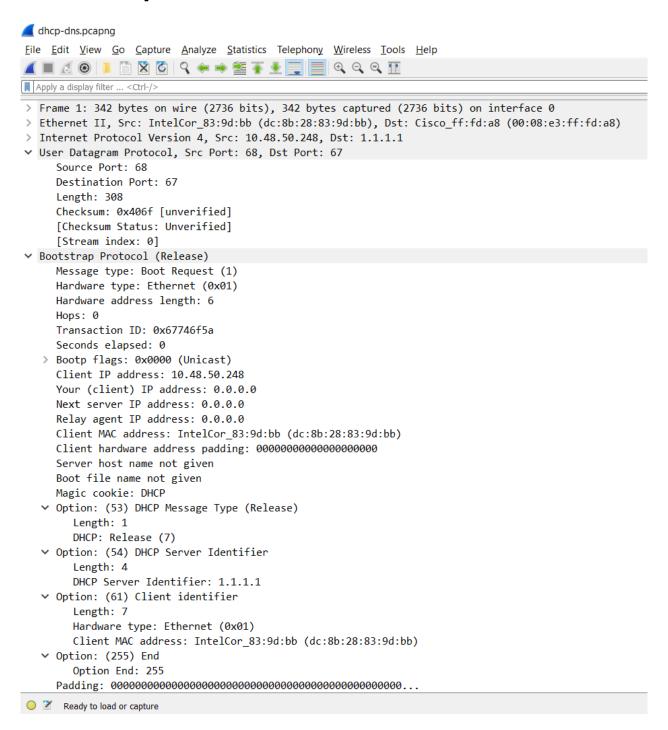


Fig 1.1 DHCP release

Ida Leung Page 2 of 14

✓ Wireshark · Packet 44 · dhcp-dns.pcapng

```
> Frame 44: 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits) on interface 0
> Ethernet II, Src: IntelCor_83:9d:bb (dc:8b:28:83:9d:bb), Dst: Broadcast (ff:ff:ff:ff:ff)
> Internet Protocol Version 4, Src: 0.0.0.0, Dst: 255.255.255

✓ User Datagram Protocol, Src Port: 68, Dst Port: 67
    Source Port: 68
    Destination Port: 67
    Length: 308
    Checksum: 0x5807 [unverified]
     [Checksum Status: Unverified]
     [Stream index: 11]
Bootstrap Protocol (Discover)
    Message type: Boot Request (1)
    Hardware type: Ethernet (0x01)
    Hardware address length: 6
    Hops: 0
    Transaction ID: 0xad0d7c67
    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: IntelCor_83:9d:bb (dc:8b:28:83:9d:bb)
    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: IntelCor_83:9d:bb (dc:8b:28:83:9d:bb)

→ Option: (50) Requested IP Address

       Length: 4
       Requested IP Address: 10.48.50.248
  ∨ Option: (12) Host Name
       Length: 3
       Host Name: MSI

→ Option: (60) Vendor class identifier
```

Fig 1.2 DHCP discover

Ida Leung Page 3 of 14

```
✓ Wireshark · Packet 44 · dhcp-dns.pcapng
```

```
Relay agent IP address: 0.0.0.0
  Client MAC address: IntelCor_83:9d:bb (dc:8b:28:83:9d:bb)
  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: IntelCor_83:9d:bb (dc:8b:28:83:9d:bb)

∨ Option: (50) Requested IP Address
     Length: 4
     Requested IP Address: 10.48.50.248

∨ Option: (12) Host Name

     Length: 3
     Host Name: MSI

→ Option: (60) Vendor class identifier

     Length: 8
     Vendor class identifier: MSFT 5.0

∨ Option: (55) Parameter Request List
     Length: 14
     Parameter Request List Item: (1) Subnet Mask
     Parameter Request List Item: (3) Router
     Parameter Request List Item: (6) Domain Name Server
     Parameter Request List Item: (15) Domain Name
     Parameter Request List Item: (31) Perform Router Discover
     Parameter Request List Item: (33) Static Route
     Parameter Request List Item: (43) Vendor-Specific Information
     Parameter Request List Item: (44) NetBIOS over TCP/IP Name Server
     Parameter Request List Item: (46) NetBIOS over TCP/IP Node Type
     Parameter Request List Item: (47) NetBIOS over TCP/IP Scope
     Parameter Request List Item: (119) Domain Search
     Parameter Request List Item: (121) Classless Static Route
     Parameter Request List Item: (249) Private/Classless Static Route (Microsoft)
     Parameter Request List Item: (252) Private/Proxy autodiscovery

∨ Option: (255) End

     Option End: 255
```

Fig 1.3 DHCP discover options

Ida Leung Page 4 of 14

```
Wireshark - Packet 45 - dhcp-dns.pcapng
 > Frame 45: 370 bytes on wire (2960 bits), 370 bytes captured (2960 bits) on interface 0
  > Ethernet II, Src: Cisco 69:bd:f0 (cc:16:7e:69:bd:f0), Dst: IntelCor_83:9d:bb (dc:8b:28:83:9d:bb)
  Internet Protocol Version 4, Src: 1.1.1.1, Dst: 10.48.50.248
 User Datagram Protocol, Src Port: 67, Dst Port: 68
      Source Port: 67
      Destination Port: 68
      Length: 336
      Checksum: 0xaf7c [unverified]
       [Checksum Status: Unverified]
      [Stream index: 0]

→ Bootstrap Protocol (Offer)

      Message type: Boot Reply (2)
      Hardware type: Ethernet (0x01)
      Hardware address length: 6
      Hops: 0
      Transaction ID: 0xad0d7c67
      Seconds elapsed: 0
    > Bootp flags: 0x0000 (Unicast)
      Client IP address: 0.0.0.0
      Your (client) IP address: 10.48.50.248
       Next server IP address: 0.0.0.0
       Relay agent IP address: 0.0.0.0
       Client MAC address: IntelCor_83:9d:bb (dc:8b:28:83:9d:bb)
      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: 1.1.1.1

→ Option: (51) IP Address Lease Time

         Length: 4
         IP Address Lease Time: (1800s) 30 minutes
    ∨ Option: (1) Subnet Mask
         Length: 4
         Subnet Mask: 255.255.248.0
    ∨ Option: (3) Router
         Length: 4
```

Fig 1.4 DHCP offer

Ida Leung Page 5 of 14

Wireshark · Packet 45 · dhcp-dns.pcapng

```
Transaction ID: 0xad0d7c67
  Seconds elapsed: 0
> Bootp flags: 0x0000 (Unicast)
  Client IP address: 0.0.0.0
  Your (client) IP address: 10.48.50.248
  Next server IP address: 0.0.0.0
  Relay agent IP address: 0.0.0.0
  Client MAC address: IntelCor_83:9d:bb (dc:8b:28:83:9d:bb)
  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: 1.1.1.1
∨ Option: (51) IP Address Lease Time
     Length: 4
     IP Address Lease Time: (1800s) 30 minutes

∨ Option: (1) Subnet Mask
     Length: 4
     Subnet Mask: 255.255.248.0

→ Option: (3) Router
     Length: 4
     Router: 10.48.48.1

∨ Option: (6) Domain Name Server

     Length: 12
     Domain Name Server: 142.55.100.25
     Domain Name Server: 142.55.44.25
     Domain Name Server: 142.55.136.25

∨ Option: (15) Domain Name

     Length: 19
     Domain Name: ddi.sheridanc.on.ca
∨ Option: (119) Domain Search
     Length: 23
     FQDN: ddi.sheridanc.on.ca
     FQDN: sheridanc.on.ca
∨ Option: (255) End
     Option End: 255
```

Fig 1.5 DHCP offer options

Ida Leung Page 6 of 14

✓ Wireshark · Packet 46 · dhcp-dns.pcapng

```
> Frame 46: 346 bytes on wire (2768 bits), 346 bytes captured (2768 bits) on interface 0
> Ethernet II, Src: IntelCor_83:9d:bb (dc:8b:28:83:9d:bb), 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: 312
    Checksum: 0x8154 [unverified]
     [Checksum Status: Unverified]
     [Stream index: 11]

→ Bootstrap Protocol (Request)

    Message type: Boot Request (1)
    Hardware type: Ethernet (0x01)
    Hardware address length: 6
    Hops: 0
    Transaction ID: 0xad0d7c67
    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: IntelCor_83:9d:bb (dc:8b:28:83:9d:bb)
    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: IntelCor_83:9d:bb (dc:8b:28:83:9d:bb)

	✓ Option: (50) Requested IP Address

       Length: 4
       Requested IP Address: 10.48.50.248

→ Option: (54) DHCP Server Identifier

       Length: 4
       DHCP Server Identifier: 1.1.1.1
  ∨ Option: (12) Host Name
```

Fig 1.6 DHCP request

Ida Leung Page 7 of 14

```
■ Wireshark · Packet 46 · dhcp-dns.pcapnq
```

```
DHCP: Request (3)

→ Option: (61) Client identifier

     Length: 7
     Hardware type: Ethernet (0x01)
     Client MAC address: IntelCor 83:9d:bb (dc:8b:28:83:9d:bb)

✓ Option: (50) Requested IP Address
     Length: 4
     Requested IP Address: 10.48.50.248

→ Option: (54) DHCP Server Identifier

     Length: 4
     DHCP Server Identifier: 1.1.1.1
∨ Option: (12) Host Name
     Length: 3
     Host Name: MSI

→ Option: (81) Client Fully Qualified Domain Name
     Length: 6
  > Flags: 0x00
     A-RR result: 0
     PTR-RR result: 0
     Client name: MSI

✓ Option: (60) Vendor class identifier
     Length: 8
     Vendor class identifier: MSFT 5.0

→ Option: (55) Parameter Request List

     Length: 14
     Parameter Request List Item: (1) Subnet Mask
     Parameter Request List Item: (3) Router
     Parameter Request List Item: (6) Domain Name Server
     Parameter Request List Item: (15) Domain Name
     Parameter Request List Item: (31) Perform Router Discover
     Parameter Request List Item: (33) Static Route
     Parameter Request List Item: (43) Vendor-Specific Information
     Parameter Request List Item: (44) NetBIOS over TCP/IP Name Server
     Parameter Request List Item: (46) NetBIOS over TCP/IP Node Type
     Parameter Request List Item: (47) NetBIOS over TCP/IP Scope
     Parameter Request List Item: (119) Domain Search
     Parameter Request List Item: (121) Classless Static Route
     Parameter Request List Item: (249) Private/Classless Static Route (Microsoft)
     Parameter Request List Item: (252) Private/Proxy autodiscovery

∨ Option: (255) End

     Option End: 255
```

Fig 1.7 DHCP offer options

Ida Leung Page 8 of 14

✓ Wireshark · Packet 47 · dhcp-dns.pcapng

```
> Frame 47: 370 bytes on wire (2960 bits), 370 bytes captured (2960 bits) on interface 0
> Ethernet II, Src: Cisco_69:bd:f0 (cc:16:7e:69:bd:f0), Dst: IntelCor_83:9d:bb (dc:8b:28:83:9d:bb)
> Internet Protocol Version 4, Src: 1.1.1.1, Dst: 10.48.50.248

∨ User Datagram Protocol, Src Port: 67, Dst Port: 68
     Source Port: 67
    Destination Port: 68
     Length: 336
     Checksum: 0xac7c [unverified]
     [Checksum Status: Unverified]
     [Stream index: 0]
Bootstrap Protocol (ACK)
     Message type: Boot Reply (2)
     Hardware type: Ethernet (0x01)
     Hardware address length: 6
    Hops: 0
    Transaction ID: 0xad0d7c67
     Seconds elapsed: 0
  > Bootp flags: 0x0000 (Unicast)
     Client IP address: 0.0.0.0
     Your (client) IP address: 10.48.50.248
     Next server IP address: 0.0.0.0
     Relay agent IP address: 0.0.0.0
     Client MAC address: IntelCor_83:9d:bb (dc:8b:28:83:9d:bb)
     Server host name not given
     Boot file name not given
    Magic cookie: DHCP
  ∨ Option: (53) DHCP Message Type (ACK)
       Length: 1
       DHCP: ACK (5)

→ Option: (54) DHCP Server Identifier
       Length: 4
       DHCP Server Identifier: 1.1.1.1
  ∨ Option: (51) IP Address Lease Time
       Length: 4
       IP Address Lease Time: (1800s) 30 minutes
  ∨ Option: (1) Subnet Mask
       Length: 4
       Subnet Mask: 255.255.248.0
  ∨ Option: (3) Router
       Length: 4
```

Fig 1.8 DHCP acknowledge

Ida Leung Page 9 of 14

```
■ Wireshark · Packet 47 · dhcp-dns.pcapng
```

```
Transaction ID: 0xad0d7c67
  Seconds elapsed: 0
> Bootp flags: 0x0000 (Unicast)
  Client IP address: 0.0.0.0
  Your (client) IP address: 10.48.50.248
  Next server IP address: 0.0.0.0
  Relay agent IP address: 0.0.0.0
  Client MAC address: IntelCor_83:9d:bb (dc:8b:28:83:9d:bb)
  Server host name not given
  Boot file name not given
  Magic cookie: DHCP

→ Option: (53) DHCP Message Type (ACK)

     Length: 1
     DHCP: ACK (5)

→ Option: (54) DHCP Server Identifier

     Length: 4
     DHCP Server Identifier: 1.1.1.1
∨ Option: (51) IP Address Lease Time
     Length: 4
     IP Address Lease Time: (1800s) 30 minutes

∨ Option: (1) Subnet Mask
     Length: 4
     Subnet Mask: 255.255.248.0

→ Option: (3) Router
     Length: 4
     Router: 10.48.48.1

∨ Option: (6) Domain Name Server

     Length: 12
     Domain Name Server: 142.55.100.25
     Domain Name Server: 142.55.44.25
     Domain Name Server: 142.55.136.25

∨ Option: (15) Domain Name

     Length: 19
     Domain Name: ddi.sheridanc.on.ca
∨ Option: (119) Domain Search
     Length: 23
     FQDN: ddi.sheridanc.on.ca
     FQDN: sheridanc.on.ca
∨ Option: (255) End
     Option End: 255
```

Fig 1.9 DHCP acknowledge options

Ida Leung Page 10 of 14

```
Wireshark - Packet 109 - dhcp-dns.pcapng
  > Frame 109: 83 bytes on wire (664 bits), 83 bytes captured (664 bits) on interface 0
 Ethernet II, Src: IntelCor_83:9d:bb (dc:8b:28:83:9d:bb), Dst: Cisco_ff:fd:a8 (00:08:e3:ff:fd:a8)
    > Destination: Cisco_ff:fd:a8 (00:08:e3:ff:fd:a8)
    > Source: IntelCor_83:9d:bb (dc:8b:28:83:9d:bb)
       Type: IPv4 (0x0800)
 Internet Protocol Version 4, Src: 10.48.50.248, Dst: 142.55.100.25
       0100 .... = Version: 4
       .... 0101 = Header Length: 20 bytes (5)
    > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
      Total Length: 69
      Identification: 0x7bac (31660)
    > Flags: 0x0000
       Time to live: 128
       Protocol: UDP (17)
       Header checksum: 0x0000 [validation disabled]
       [Header checksum status: Unverified]
       Source: 10.48.50.248
       Destination: 142.55.100.25
 User Datagram Protocol, Src Port: 61570, Dst Port: 53
       Source Port: 61570
      Destination Port: 53
      Length: 49
       Checksum: 0x2fbb [unverified]
       [Checksum Status: Unverified]
       [Stream index: 20]

→ Domain Name System (query)

       Transaction ID: 0x9605
    > Flags: 0x0100 Standard query
       Questions: 1
       Answer RRs: 0
       Authority RRs: 0
       Additional RRs: 0
    V Oueries
       dm2305.storage.live.com: type A, class IN
            Name: dm2305.storage.live.com
            [Name Length: 23]
            [Label Count: 4]
            Type: A (Host Address) (1)
            Class: IN (0x0001)
       [Response In: 110]
```

Fig 1.10 DNS request

Ida Leung Page 11 of 14

✓ Wireshark · Packet 110 · dhcp-dns.pcapng

```
> Frame 110: 287 bytes on wire (2296 bits), 287 bytes captured (2296 bits) on interface 0
Ethernet II, Src: Cisco_ff:fd:a8 (00:08:e3:ff:fd:a8), Dst: IntelCor_83:9d:bb (dc:8b:28:83:9d:bb)
  > Destination: IntelCor_83:9d:bb (dc:8b:28:83:9d:bb)
  > Source: Cisco_ff:fd:a8 (00:08:e3:ff:fd:a8)
    Type: IPv4 (0x0800)

▼ Internet Protocol Version 4, Src: 142.55.100.25, Dst: 10.48.50.248

    0100 .... = Version: 4
     .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 273
     Identification: 0x68e9 (26857)
  > Flags: 0x0000
    Time to live: 61
    Protocol: UDP (17)
    Header checksum: 0xe47a [validation disabled]
     [Header checksum status: Unverified]
    Source: 142.55.100.25
    Destination: 10.48.50.248
Source Port: 53
    Destination Port: 61570
    Length: 253
    Checksum: 0x2c1d [unverified]
     [Checksum Status: Unverified]
     [Stream index: 20]

∨ Domain Name System (response)

    Transaction ID: 0x9605
  > Flags: 0x8180 Standard query response, No error
    Questions: 1
    Answer RRs: 5
    Authority RRs: 0
    Additional RRs: 0

√ dm2305.storage.live.com: type A, class IN

          Name: dm2305.storage.live.com
          [Name Length: 23]
          [Label Count: 4]
          Type: A (Host Address) (1)
          Class: IN (0x0001)
  > Answers
     [Request In: 109]
```

Fig 1.11 DNS response

Ida Leung Page 12 of 14

Step 3: Answer the following questions based on your finding.

DHCP Protocol

1. What address is being used for DHCP request as source? Why it is being used? What address is being used for the DHCP rekmZquest as destination? Why it is being used?

Source address: 0.0.0.0

Destination address: 255.255.255.255

When every network follows same standards then we don't need to remember settings for each network connection. So, by default when you are trying to connect network, your system send request using first IP. Same for destination address. It sends request using broadcast network address.

2. What is the lease timer for your IP? In which DHCP option you can locate it?

Option(51): IP Address Lease Time

Duration: (1800s) 30 minutes

3. What do the four basic information require for your laptop to access to Internet? Where can you locate that information from the DHCPOFFER? (i.e. which option)

Option(3) Router: 10.48.48.1

Option(6) Domain Name Server: 142.55.100.25

Client IP address: 10.48.50.248

Option(51) IP Address Lease Time: 30 minutes

4. What is the port number for the server end?

Port number: 67

Ida Leung Page 13 of 14

DNS Protocol

1. What is the DNS server IP? Where do you obtain the DNS server IP?

Obtain it from DHCP server when you request for new IP address

IP address: 142.55.100.25 142.55.44.25

142.55.136.25

2. What is the destination mac address on your DNS request? How do your laptop find out the mac address?

Destination MAC address: 00:08:e3:ff:fd:a8 Laptop find that mac address using ARP and RARP which discovers from IP address given by DHCP server.

3. Disable the wireless/wireline connection, do nslookup www.youtube.com in command prompt. Keep the wireshark running. Do you able to resolve the youtube.com domain name? If so, how? If not, what happen after the first DNS request out without response?

No, unable to resolve server for youtube.com. Basically, you don't get response from server. Since DNS request follows UDP protocol, it doesn't care to wait for DNS response.

4. What is in common for DHCP and DNS request (in terms of transport layer)? Why? What are the differences? (in terms of delivery methodology such as unicast, multicast, broadcast) Why?

Common: none Difference:

- Destination port for DHCP is 67 and DNS is 53
- DHCP request uses TCP protocol and DNS uses UDP protocol
- 5. What is the port number for the server end?

Port: 53

Ida Leung Page 14 of 14