|  |  |  |
| --- | --- | --- |
| **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

# 

# Fig 1.2 DHCP discover

# 

# Fig 1.3 DHCP discover options

# 

# Fig 1.4 DHCP offer

# 

# Fig 1.5 DHCP offer options

# 

# Fig 1.6 DHCP request

# 

# Fig 1.7 DHCP offer options

# 

# Fig 1.8 DHCP acknowledge

# 

# Fig 1.9 DHCP acknowledge options

# 

# Fig 1.10 DNS request

# 

# Fig 1.11 DNS response

# 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

1. 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

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

Port number : 67

## 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

1. 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.

1. Disable the wireless/wireline connection, do nslookup [www.youtube.com](http://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.

1. 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

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

Port : 53