Experiment No. : 09 Date : 06-5-2024

Problem statement

Trace Packets using Wireshark for DNS and answer the following Questions.

Use this URL http://www.ietf.org

1 Locate the DNS query and response messages. Are they sent over UDP or TCP?

→ They are sent over UDP

2 What is the destination port for the DNS query message? What is the source port of DNS response message.

→ The destination port for the DNS query message is 53
The source port of DNS response message is 83

3 To what IP address is the DNS query message sent? Use ipconfig to determine the IP address of your local DNS server. Are these two IP address the same.

→ It is sent to 204.57.180 which is the IP address of one of my local DNS server.

4 Examine the DNS query message. What "Type" of DNS query is it? Does the query message contain any answers.

→ It is a "Type" of standard query.
And it doesn't contain any answers.

Experiment No. : ..... Date : .....

5 Examine the DNS response message. How many "answers" are provided? What does each of the answers contain?

→ There were 1 answer containing information about: www.ietf.org: type A, class IN, addr 204.173.57.180

Name : www.ietf.org

Type : A (Host address) class : IN (0x0001)

Time to live : 30 minutes

Data length : 4

6 Consider the subsequent TCP SYN packet sent by your host. Does the destination IP address of the SYN packet correspond to any of the IP addresses provided in the DNS response message?

→ The first SYN packet was sent to 204.173.57.180 which corresponds to the first IP address provided in the DNS response message.

7 This web page contains image. Before retrieving each image, does your host issues new DNS queries

→ No

Use nslookup -type = NS mit.edu

Experiment No. :..... Date :.....

8. To what IP address is the DNS query message sent? Is this the IP address of your default local DNS server?

→ It is sent to 192.168.1.1 and is the default local DNS server.

9. Examine the DNS query message what "Type of DNS query is it? Does the query message contain any answers?

→ The query is of type A and it doesn't contain any answers.

10. Examine the DNS response message. What MIT name servers does the response message provide? Does this response message also provide the IP addresses of the MIT name servers?

→ Name : www.mit.edu

Type : A (Host address)

class :

IN (0x0001)

Time to live : 1 minute

Data length = 4

Addr : 18.7.22.83

Experiment No.: 10

Date: 06-05-2024

Problem statement

Trace packets using wireshark for DHCP and answer the following questions

Use ipconfig/release and ipconfig/renew commands

1. Are DHCP message sent over UDP or TCP ?

→ The DHCP messages are sent via UDP

2. What is the link-layer (e.g Ethernet) address of your host?

→ The ethernet address of my host is 00:0f:66:52:a6:33

3. What is the value DHCP discover message differentiate this message from the DHCP request message ?

→ DHCP message type

Request includes a server identifier field

4. What is the value of the Transaction-ID in each of the first four discover/offer/Request/ACK DHCP message? What are the value of the Transaction-ID in the second set (Request/ACK) of DHCP message? What is the purpose of the Transaction-ID field ?

→ 1st set of messages : 0x6fd4bb

2nd set of messages : 0x53a63280

Purpose : The transaction ID is different so that the host can differentiate between different requests made by the user.

Experiment No.

Date :

5 A host uses DHCP to obtain an IP address, among other things. But a host's IP address is not confirmed until the end of the four-msg exchange, IP the IP address is not set until the end of the four-message exchange. Then what values are used in the IP datagram in the four-msg exchange? For each of the four DHCP msg indicate the source & dest IP address that are carried in the encapsulating IP datagram.

→ Discover : 000.0/255.255.255.255.
Offer : 192.168.1.1/255.255.255.255
Request : 0.0.0.0/255.255.255.255
ACK : 192.168.1.1/255.255.255.255

6 What is the IP address of your DHCP server?

→ 192.168.1.1

7 What IP address is the DHCP server offering to your host in the DHCP offer message? Indicate which DHCP message contains the offered DHCP address

→ My client is offered 192.168.1.10 by DHCP server. The offer message contains the DHCP address offered by the server

8 What values in the trace indicate the absence of a relay agent? Is there a relay agent in your experiment? If so what is the IP address of agent?

→ The value indicates there is no relay agent 0.0.0.0

eriment No. :..... Date :.....

Explain the purpose of the lease time. What is the lease time value in your experiment?

→ * The purpose of the lease time is to tell the client how long they can use the specific IP address assigned by the server before they will have to be assigned a new one.
* The lease time in my experiment is 86400 seconds or 1 day

What is the purpose of the DHCP release message? Does the DHCP server issue an acknowledgment of receipt of the client's DHCP request?

→ * The purpose of the release messages is to release the IP address back to the server
* There is no verification that the release message has been received by the server.

Experiment No. : 06 Date : 1/04/2024

Problem Statement

Trace packets using Wireshark for HTTP and Answer the following Questions.

The Basic HTTP GET/response interaction

Use URL : http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html

1 Is your browser running HTTP version 1.0 or 1.1 ? What version of HTTP is the server running ?

→ Browser — HTTP 1.1 version

Server — HTTP 1.1 version

2 What languages does your browser indicate that it can accept from the server ?

→ en-US, en; q=0.5\r\n

3 What is the status code returned from the server to your browser ?

→ Status code : 200

4 When was the HTML file, that you are retrieving last modified at the server

If-Modified-Since : Mon, 01 Apr 2024 05:59:02 GMT\r\n

5 How many bytes of content are being returned to your browser

→ 128 bytes of content are being returned.

Experiment No. :..... Date :.....

The HTTP CONDITIONAL GET / response interaction

URL : http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html

6 Inspect the contents of the first HTTP GET request from your browser to the server? Do see an "IF-MODIFIED-SINCE" line in the HTTP GET ?

→ No there is no IF-MODIFIED-SINCE line in GET any

7 Inspect the contents of the server response. Did the server explicitly return the contents of the file ? How can you tell ?

→ The server did explicitly return the contents of the file. Wireshark includes a section title "line-Based Text Data" which shows what the server sent back to my browser which is specifically what the website showed when I brought it on my browser

8 Now inspect the contents of the second HTTP GET request from your browser to the server. Do you see an "IF-MODIFIED-SINCE." line in the HTTP GET ? If so, what information follows the "IF-MODIFIED-SINCE", header ?

→ Yes in the second HTTP message an "IF-MODIFIED-SINCE line is included. The information that follows is the data and time that I accessed the webpage

Experiment No. :..... Date :.....

9 What is the HTTP status code and phrase returned from the server in response to the second HTTP GET ? Did the server explicitly return the contents of the file ? Explain

→ The HTTP status code is "304 : Not Modified"
The server did not return

Experiment No. : 07 Date : 7-04-2024

Problem statement

Trace packets using Wireshark for HTTP and answer the following questions for retrieving long documents

URL : http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-files.html

1 How many HTTP GET request message were sent by your browser ?

→ My browser sent 2 HTTP-GET request to the server, The packet contain GET message with packet number 16050, 16428

2 How many data containing TCP segments were needed to carry the single HTTP Responses ?

→ The data was sent in 2 TCP segments to the browser to carry the single HTTP Response and then reasembled

3 What is the status code and phrase associated with the reponse to the HTTP GET Request

→ The status code 200 with phrase OK

4 Are there any HTTP status lines in the transmitted data associated with a TCP reassembled segment of a PDU ?

Experiment No. :..... Date :.....

For HTML Documents with Embedded Objects use

URL : http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file4.html

5 How many HTTP GET request messages were sent by your browser? To which Internet address were these GET requests sent?

→ My browser sent 2 HTTP GET requests messages. One each to each for each of the following

* Initial Page Address
* Pearson Logo :
* Pearson book, 5th Edition :

6 Can you tell whether your browser downloaded the two images serially or whether they were downloaded from the two web sites in parallel? Explain

→ The browser downloaded the two images in serial order. I belive this to be the case because the first image was requested and sent before the second image was requested by the browser. Had they been running in parallel, both files would have been returned in the same time period. In this case however, the second image was only requested.

Experiment No. :..... Date :.....

For HTTP Authentication use

Username : wireshark-students Password : "network"

URL : http://gaia.cs.umass.edu/wireshark-labs/protected_pages/HTTP-wireshark-file5.html

7 What is the server's response (status code and phrase) in response to the initial HTTP GET message from your browser?

→ The server initial response was "401 Authentication Required"

8 When does your browser send the HTTP GET message for the second time, what new field is included in the HTTP GET message?

→ The new field is now included is the authorization field. This is included because we sent the server a username and password along with our request stating that were authorized to receive the page.

Experiment No. : 08 Date : 15-04/2024

Problem statement

Trace packets using wireshark for IP, ICMP and Answers the following Questions :

Use the following command to change the ICMP packet size

Ping <ipaddress/url> -s <packet size>

example : ping makemytrip.com -s 2000

1 Select the first ICMP Echo Request message sent by your computer, and expand the Internet Protocol part of the packet in the packet details window. What is the IP address of your computer ?

→

2 Within the IP packet header, what is the value in the upper layer protocol field ?

→ Within the header, the value of upper layer protocol field is ICMP (1)

3 How many bytes are in the IP header ? How many bytes are in the payload of the IP datagram ? Explain how you determined the number of payload bytes.

→ IP header length = 20 bytes

Payload = Total length - IP header length

= 84 - 20

= 64 bytes

Experiment No. :..... Date :.....

Therefore, there are 20 bytes in IP header and 8th bytes of total length, this gives the payload of the IP datagram.

4 Has this IP datagram been fragmented? Explain how you determined whether or not the datagram has been fragmented?

→ The more fragments bit = 0, so the data is not fragmented.

5 Which fields in the IP datagram always change from one datagram to the next within this series of ICMP message sent by your computer?

→ Identification, Time to live and Header checksum always change.

6 Which field stay constant?

→ The fields that stay constant across the IP datagram are:

* Version
* Header length
* Source IP
* Destination IP
* Upper layer protocol

7 Find the first ICMP Echo Request message that was sent by your computer after you changed the packet size to be 2000. Has that message been fragmented across more than one IP datagram?

→ Yes, this packet has been fragmented across more than one IP datagram

Experiment No. :..... Date :.....

8 Write the first fragment of the fragmented IP datagram. What information in the IP header indicates that the datagram has been fragmented? What information in the IP header indicates whether this is the first fragment versus a latter fragment? How long is this IP datagram?

→ The flag bit for more fragments is set, indicating that the datagram has been fragmented. Since the fragment offset is 0, we know that this is the first fragment. The first datagram has a total length of 1500, including the header.

9 What information in the IP header indicates that this is not the first datagram fragment? Are there more fragments? How can you tell?

→ We can tell that this is not the first fragment, since the fragment offset is 1480. It is the last fragment, since the more fragments flag is not set.

10 What fields change in the IP header between the first and second fragment?

→ The IP header fields that changed between the fragments are: total length, flags, fragment offset and checksum

Experiment No. : 04 Date : 18/03/2024

Problem Statement

Design and simulate a wireless network in Adhoc mode with combinations for enabling and disabling RTS/CTS and fragmentation. Observe its performance w.r.t end-to-end delay, throughput, and packet delay ratio.

Algorithm

i) Network Topology Design - nodes communicating in Ad-hoc mode

ii) Node configuration - MAC layer settings such as RTS/CTS and fragmentation threshold

iii) Enable/Disable RTS/CTS and fragmentation

iv) Traffic generation

v) performance metrics

vi) simulation execution

vii) Analysis

Program

```
#include "ns3/internet-module.h"
#include "ns3/network-module.h"
#include "ns3/applications-module.h"
#include "ns3/core-module.h"
#include "ns3/config.h"
#include "ns3/double.h"
```

Experiment No. : 05 Date : 18/03/2024

Problem Statement

Create a wireless network to implement AODV routing protocol and observer the number of packets sent and received with the parameter throughput, delay, packet loss.

Algorithm

i) Network Topology Design

ii) Node Configuration

iii) Traffic Generation

iv) Performance metrics

v) simulation Execution

vi) Analysis

Program

```
#include "ns3/internet-module.h"
#include "ns3/network-module.h"
#include "ns3/applications-module.h"
#include "ns3/core-module.h"
#include "ns3/config.h"
#include "ns3/double.h"
#include "ns3/internet-stack-helper.h"
#include "ns3/ipv4-address-helper.h"
```

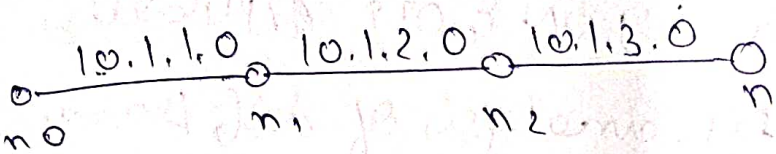
Lab program 1

Problem statement

Date: 26/02/24

wired network with constant Bit rate (CBR) data transmission over UDP's possible lab can be based on designing and simulation a wired network with duplex links between 'n' nodes with CBR over UDP. Set the queue size, vary the bandwidth and analyse the performance.

network topology



Point - to - Point

Commands

```
$ cd Downloads/
$ cd ns3.2024
$ ls
$ cd ns-allinone-3.41/
$ ls
$ cd ns-3.41
$ cp ocamples/traffic-control/traffic-control.cc
                    scratch/

$ cd scratch
$ ls
$ gedit traffic-control.cc
```

Algorithm

Step 1: Creating 'n' nodes

Step 2: Configure of Data link layer
(through wired or wireless)

Step 3: Configure network layer
(by Assigning IP address)

Step 4: Configure Transport layer
Specify (TPC or UDP) / both

Step 5: Sending data by ON & OFF Applications

Step 6: Performance analysis of data transmission

Code

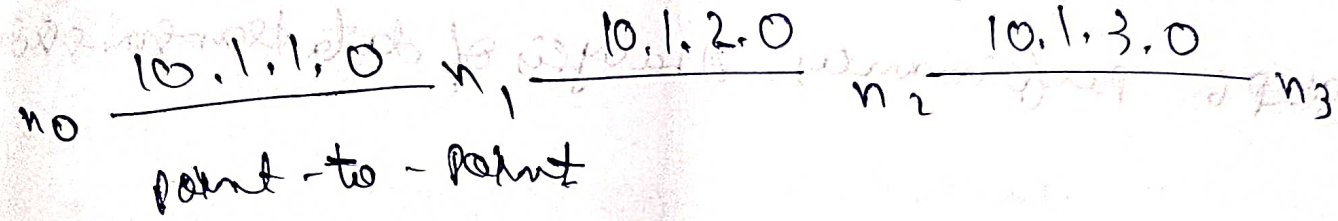
```
#include "ns3/applications-module.h"
#include "ns3/core-module.h"
#include "ns3/flow-monitor-module.h"
#include "ns3/internet-module.h"
#include "ns3/network-module.h"
#include "ns3/point-to-point-module.h"
#include "ns3/traffic-control-module.h"

using namespace ns3;

NS_LOG_COMPONENT_DEFINE ("TrafficControlExample");

void
TcPacketsInQueueTrace (uint32_t oldValue, uint32_t
                       newValue)
{
  std::cout << "TcPacketsInQueue" << oldValue
    << "to" << newValue << std::endl;
}
```

Lab Program-2 Date:- 04/03/24

Problem Statement

wired Network with Constant Bit rate (CBR) data transmission: Possible lab can be based on designing and simulating a wired network with with duplex links between 'n' nodes with CBR over UDP and TCP & the same, vary the bandwidth and analyze the performance

Network Topology



Commands

$ cd ns3-2024/
$ cd ns-allinone-3.41/
$ cd ns-3.41/
$ cp scratch/traffic-control.cc scratch/lab2.cc
$ ls scratch/
$ gedit scratch/lab2.cc &

to run the code

$ cd ..
$ ./ns3 run scratch/lab2

Algorithm

Step 1: Creating 'n' nodes

Step 2: Configure Data Link Layer (through wire or wireless)

Step 3: Configure Network layer (by Assigning IP address)

Step 4: Configure Transport layer (specify (TCP or UDP or both)

Step 5: Sending Data by ON and OFF applications

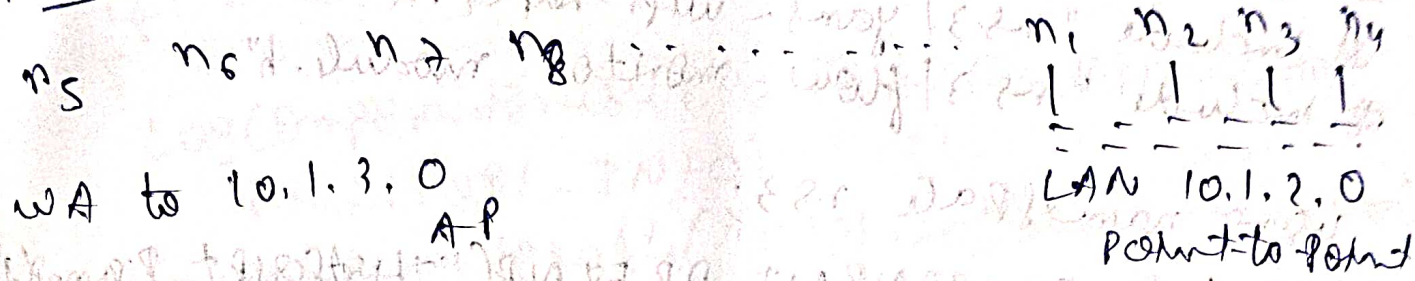
Step 6: Performance, Analysis of data transmission

```
#include "ns3/applications-module.h"
#include "ns3/core-module.h"
#include "ns3/flow-monitor-module.h"
#include "ns3/internet-module.h"
#include "ns3/network-module.h"
#include "ns3/point-to-point-module.h"
#include "ns3/traffic-control-module.h"

using namespace ns3;
NS_LOG_COMPONENT_DEFINE("TrafficControlExample");

void
TcPacketsInQueueTrace(uint32_t oldValue,
```

Program-3 Date:- 11/03/24

3) possible lab can be based on designing and simulating simple extended service set with transmitting nodes in wireless LAN & determine the performance with varying bandwidth & traffic.

network topology



Algorithm

Step1:- Creating 'n' nodes

Step2:- Configure Data link layer through wire or wireless

Step3:- Configure network layer by assigning IP address

Step4:- Configure Transport layer. Specify TCP or UDP

Step5:- Sending data by ON & OFF application

Step6:- Performance Analysis of data transmission

commands

```
$ cd ns3-2024/
$ cd ns-allinone-3.41/
$ cd ns-3.41/ - $ cd. scratch/
$ cp examples/tutorials/third.cc
$ gedit scratch/third.cc
$ cd
$ ./ns3 run scratch/third
```