REMOTE LAB

Exercise 16(b)

UDP

V1

|  |
| --- |
| Hardware List: |
| N/A |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
| Software List: |
| Protocol Analyser | Wireshark | Current Version |  |
| Frame Generator | Ostinato | Current Version |  |
|  |  |  |  |
| Remote Lab PC: | N/A | Remote Lab Type: | D |

RRRemote Lab Type: A-EIT PC with hardware, B-EIT PC with Simulation Software, C-Cloud PC with software, D-Student/Home PC

|  |  |  |  |
| --- | --- | --- | --- |
| Created By: | DR | Date: | 23/02/14 |
| Checked By: | DS | Date: | 14/11/2015 |
| Released on: | 14/11/2015 | Next Review Date: |  |



**Objective**

To analyse the structure of a UDP packet (frame).

**Preparation**

It is assumed that you already have Wireshark installed.

1. Download Ostinato (*ostinato-bin-win32-0.5.1zip*) from Moodle, or from <http://code.google.com/p/ostinato/wiki/Downloads>.
2. Unzip it (no need to install).
3. If you are interested in the Ostinato dicumentation, you will find it on the download site as well.

**Instructions**

You need administrator privileges to run Ostinato.

Run Ostinato by clicking on the executable.



The program will open.



Double-click on Port Group 0 (top left). A drop down list with available interfaces will appear. We will select the Ethernet interface (see below).



Another box will open in the top right-hand corner.

**NB Your antivirus program might object. Just tell it to allow the program to run.**





Right-click within this area. A menu will drop drown and we will select ‘New Stream’.



Double-click in the ‘Name’ field and give it any name you like.



Now, once again, right-click in this area, and select ‘Edit Stream’. Use the radio buttons to configure a packet with a hex payload, using UDP over IPv4 over Ethernet.



Click on the other tabs to check the packet composition and default parameters. Note that the default rate is 1 packet per second.

**NB DO NOT FORGET TO CLICK ‘APPLY’**

In the statstics window, select the same port (select the whole column by clicking on the column heading) for which you configured the stream (IMPORTANT).



Now click on ‘Start Tx’ in the bottom left-hand corner.

It might be a good idea to close your browser in order to reduce the amount of captured traffic.

Run Wireshark and check the bottom of the list until you see the UDP packets appearing. Then stop.

Select any of the UDP frames.



Now open up the UDP header.



Note the following:

* The source and destination ports are used for identification only (no connection)
* No handshaking
* Header length only 8 bytes (the 28 includes the 20 bytes of application data).