REMOTE LAB

Exercise 15(b)

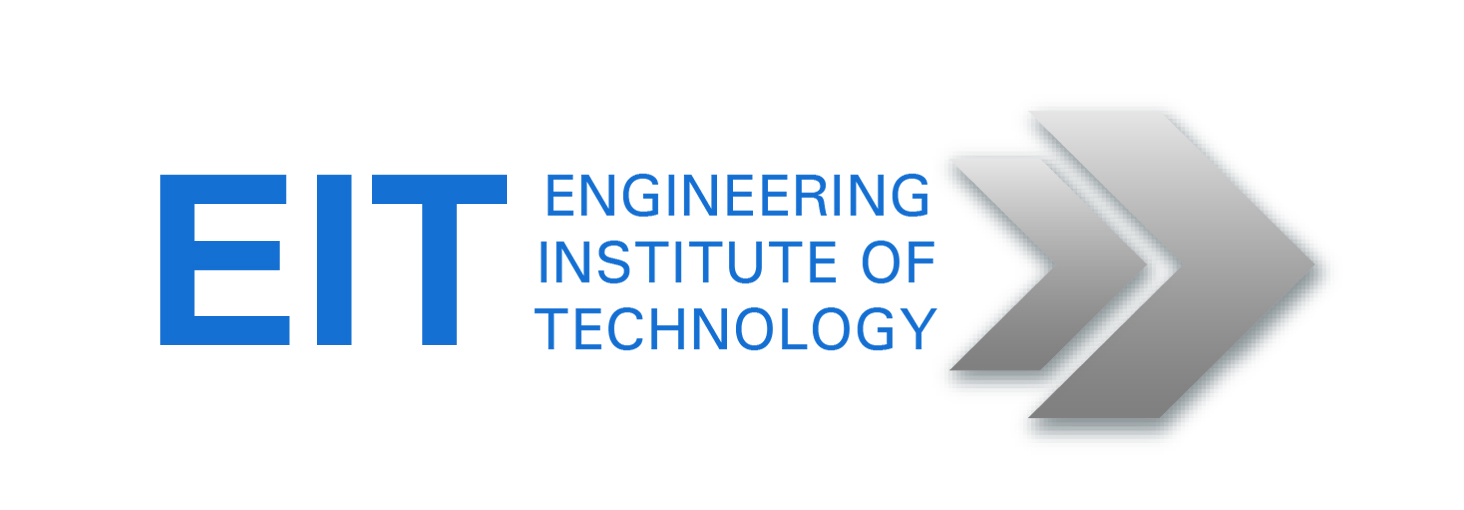
IPv6

V1

|  |  |  |  |
| --- | --- | --- | --- |
| Hardware List: | | | |
| N/A |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
| Software List: | | | |
| Protocol Analyser | Wireshark | Current Version |  |
| Frame Generator | Ostinato | Current Version |  |
|  |  |  |  |
| Remote Lab PC: | Remote Lab 1 or Self Download | 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 |
| Checked By: | JT | Date: | 17/05/2016 |



**Objective**

To analyse the structure of an IPv6 packet (frame).

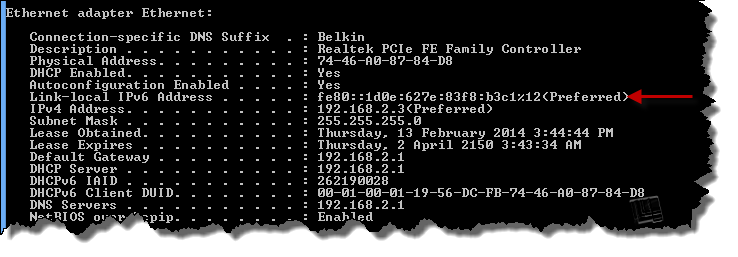
**Preparation**

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 documentation, you will find it on the download site as well.

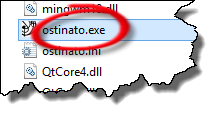
**Instructions**

First check the IPv6 address of your own computer, e.g. by using the ipconfig /all command from the command prompt, or with IP Configuration Manager or something similar.

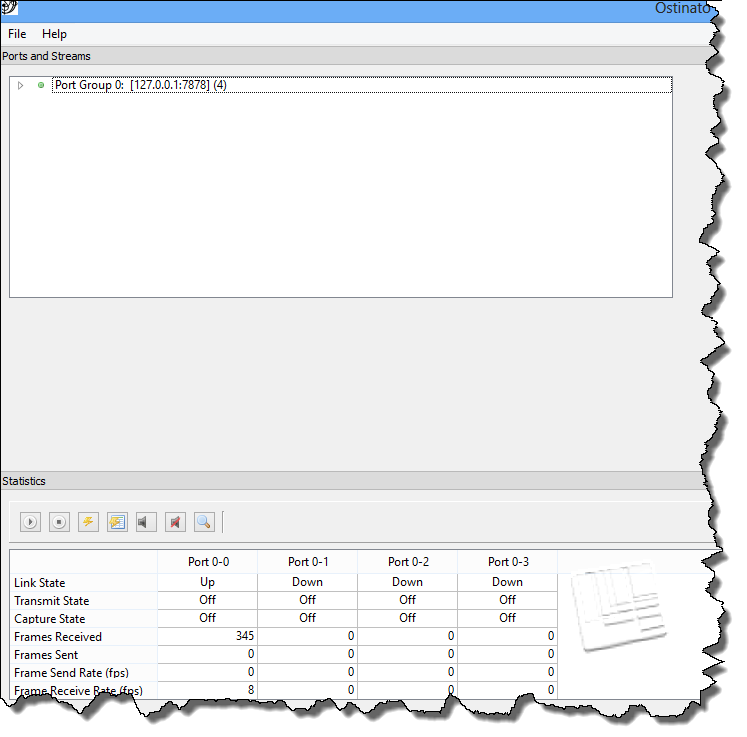


In our case the IPv6 address (on a Private network) is a Link-Local address. Apart from it eing listed as such, it is also abvious because of the fe80 at the beginning of the address. Refer to Annexure 1 for more detail in IPv6 classes.

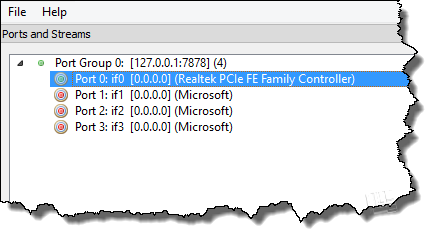
Now run Ostinato by clicking on the executable.



The program will open.



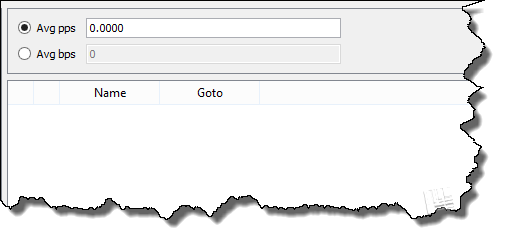
Double-click on Port Group 0 (top left). A drop down list with available interfaces will appear. We will select the Ethernet interface (see below).



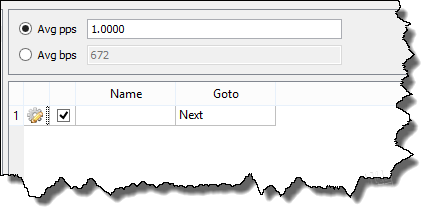
Another box will open in the top right-hand corner.

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

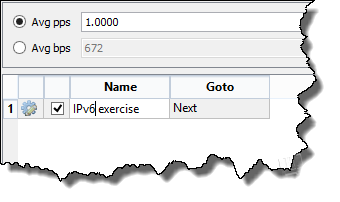




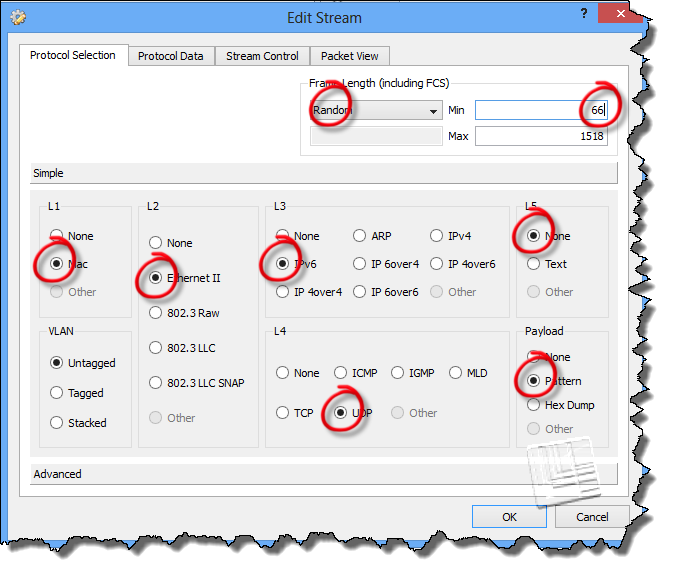
Right-click within this area. A menu will drop drown and we will select ‘New Stream’.



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



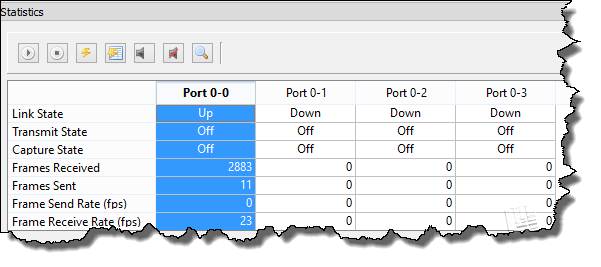
Now, once again, right-click in this area, and select ‘Edit Stream’. Use the radio buttons to configure a packet with a hex payload, using UDP over IPv6 over Ethernet.



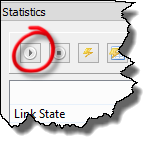
Click on the other tabs to check the packet composition and default parameters. Note that the default rate is 1 packet per second.

**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).



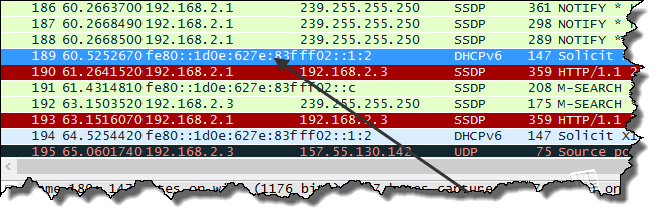
Now click on ‘Start Tx’ in the bottom left-hand corner.



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 IPv6 packets appearing. Then stop.

Select any of the IPv6 frames. Note your own IPv6 address.



Note the following:

* Version (6)
* Traffic class
* Flow label
* Payload length
* Next header (UDP)
* Hop limit
* Source IP address
* Destination IP address

Compare this with the details of the IPv4 header as captured earlier in Exercise #15.