Author : Tony Hill

Date : 11th April 2014

Version : 1-0

1 Introduction

Ostinato is a free IPv4 traffic generator tool for Windows and Linux. It is very useful for basic load testing and is capable of generating traffic volumes that approximate to the transmission bandwidth capabilities of a PC or laptop's Ethernet adapter.

It is also very useful for creating and generating packets with different layer-2, layer-3 and layer-4 content, in particular packets with different ToS and DSCP fields. This guide focuses on using Ostinato for this very purpose.

The tool can be downloaded at the following URL, which also contains links to a user guide and other useful information.

http://code.google.com/p/ostinato/

If running on Windows, it is necessary to download and install the Windows packet capture library [WinPcap] from the following URL:

http://www.winpcap.org/

Those who use Wireshark will already have WinPcap installed.

2 ToS & DSCP Values

DSCP values are specified using the six most significant bits of the DSCP byte.

2^5	2^4	2^3	2^2	2^1	2^0	ECN	ECN
32	16	8	4	2	1		
bit 6	bit 5	bit 4	bit 3	bit 2	bit 1		
class selector			drop probability		0		

Bits 6, 5 & 4 are the Class Selector (formerly known as ToS bits), bits 3 & 2 the drop probability and bit 1 is currently always zero.

Table-1 below shows the DSCP values ordered by drop probability. The bits within each class are sub-divided to determine the Assured Forwarding value. For example, AF 32 uses DSCP bits 011 10 0 where 011 = 3_{10} and 10 = 2_{10} with bit 1 = 0.

Drop Prob.	Class 0	Class 1	Class 2	Class 3	Class 4	Class 5	Class 6	Class 7
LOW	000 00 0	001 01 0	010 01 0	011 01 0	100 01 0	101 00 0	110 00 0	111 00 0
	AF	AF 11	AF 21	AF 31	AF 41			
	DSCP	10	18	26	34			
MED		001 10 0	010 10 0	011 10 0	100 10 0			
	AF	AF 12	AF 22	AF 32	AF 42			
	DSCP	12	20	28	36			
HIGH		001 11 0	010 11 0	011 11 0	100 11 0	101 11 0		
	AF	AF 13	AF 23	AF 33	AF 43	EF		
	DSCP	14	22	30	38	46		

Table-1: DSCP Values

3 Ostinato

3.1 Calculating DSCP Values

DSCP values are entered in Ostinato using all eight bits of the DCSP byte and converting from decimal to hexadecimal. Table-2 below shows the hexadecimal values in the right-most column to enter into the Ostinato DSCP configuration.

	DSCP	bit 6	bit 5	bit 4	bit 3	bit 2	bit 1	ECN	ECN		
	Value	32	16	8	4	2	1				
	Byte	bit 7	bit 6	bit 5	bit 4	bit 3	bit 2	bit 1	bit 0		
AF	Value	128	64	32	16	8	4	2	1	Dec	Hex
AF 11	10	0	0	1	0	1	0	0	0	40	28
AF 21	18	0	1	0	0	1	0	0	0	72	48
AF 31	26	0	1	1	0	1	0	0	0	104	68
AF 41	34	1	0	0	0	1	0	0	0	136	88
AF 12	12	0	0	1	1	0	0	0	0	48	30
AF 22	20	0	1	0	1	0	0	0	0	80	50
AF 32	28	0	1	1	1	0	0	0	0	112	70
AF 42	36	1	0	0	1	0	0	0	0	144	90
AF 13	14	0	0	1	1	1	0	0	0	56	38
AF 23	22	0	1	0	1	1	0	0	0	88	58
AF 33	30	0	1	1	1	1	0	0	0	120	78
AF 43	38	1	0	0	1	1	0	0	0	152	98
EF	46	1	0	1	1	1	0	0	0	184	B8

Class	Drop Prob.

Table-2: Ostinato DSCP Value Conversion

3.2 Creating Streams

In this example, I am creating a UDP stream to send to a remote device to test that packets with a specific QoS value are being generated correctly. It is also possible to capture packets using Wireshark and to import them into Ostinato to create streams.

Open Ostinato and expand the Port Group in the left-hand Ports and Streams pane. Select the interface over which you will generate traffic. This causes the stream pane to open in the top right-hand corner. If no interfaces are visible within the Port Group it is necessary to install WinPcap. You can also create additional Port Groups and place selected interfaces within the group.

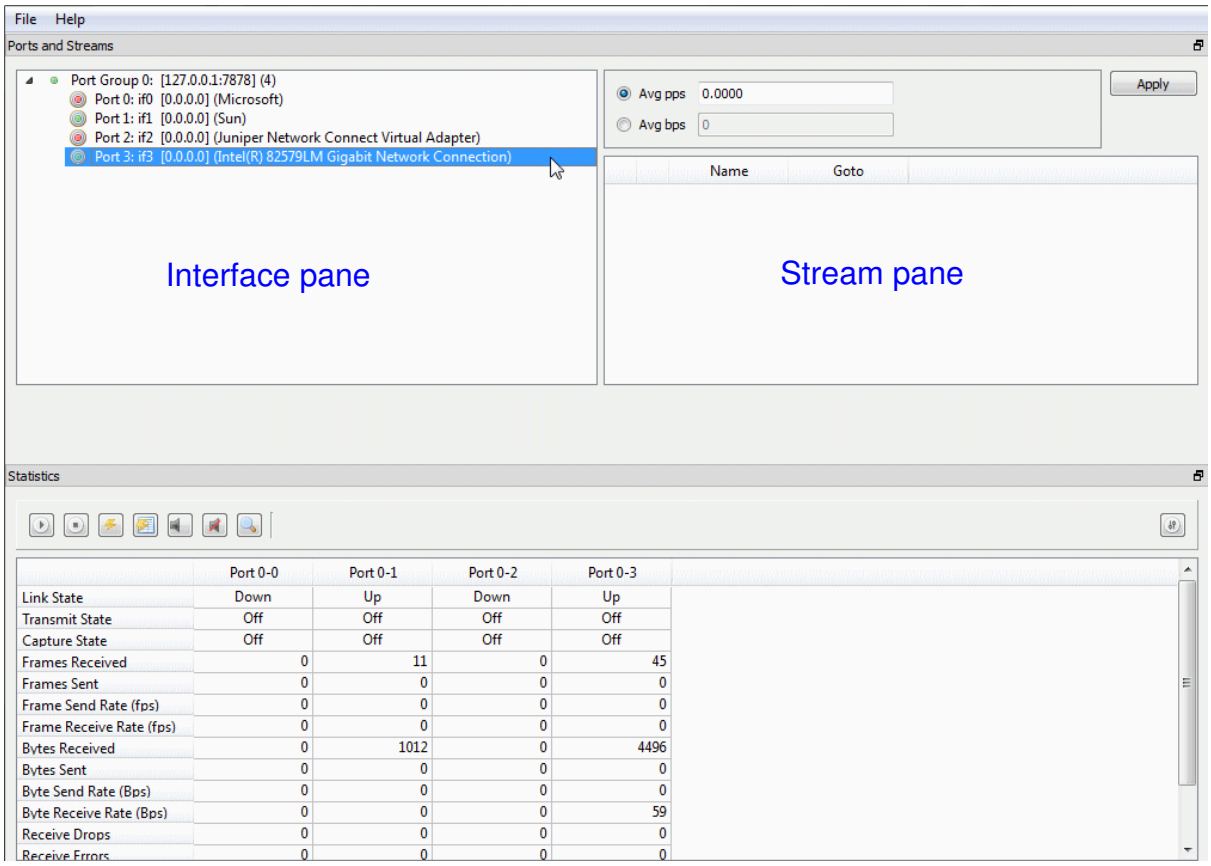


Figure-1: Select the Interface to Generate Traffic

Right-click within the stream pane and select New Stream.

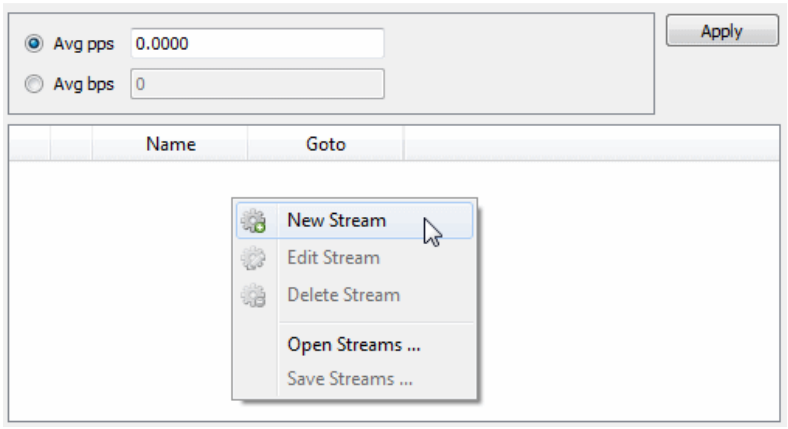


Figure-2: Create a New Stream

Select the stream and right-click, select Edit Stream.

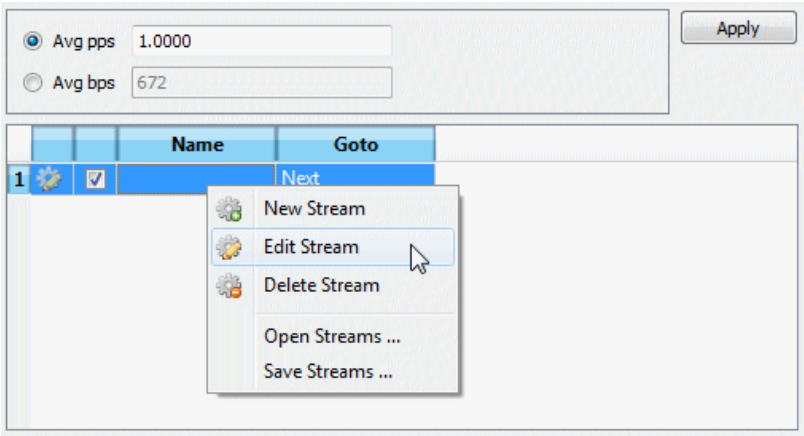


Figure-3: Edit Stream

In the Simple section of the Protocol Selection tab, select frame length (fixed, random etc.), click the radio buttons to choose L1 MAC and VLAN, L2 Ethernet type, L3 protocol, L4 protocol and L5 information. In this example I am using fixed 1,000 byte frame, untagged VLAN, Ethernet II, IPv4 with UDP and leaving the L5 defaults of None and Pattern for the payload.

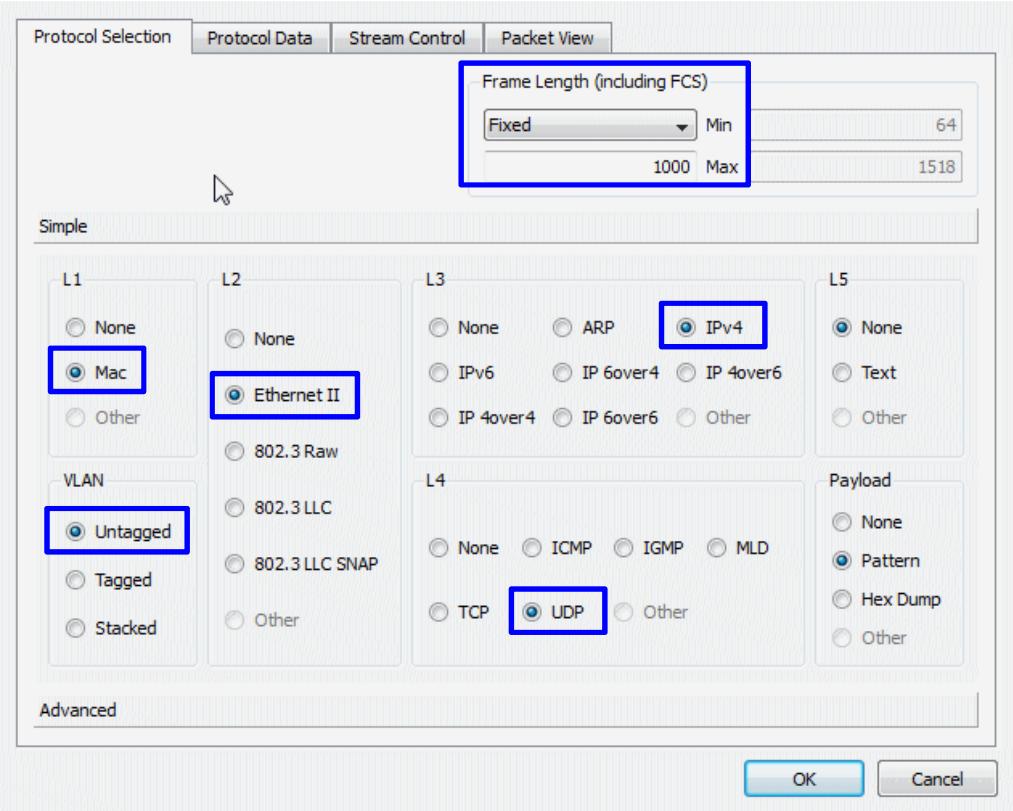


Figure-4: Protocol Selection

If you wish, select the Advanced tab at the foot of the window and insert additional fields from the Available Protocols pane on the left, such as SNAP or 802.3 LLC. These additional fields will appear in the next tab, Protocol Data. In this example I am not using any additional fields.

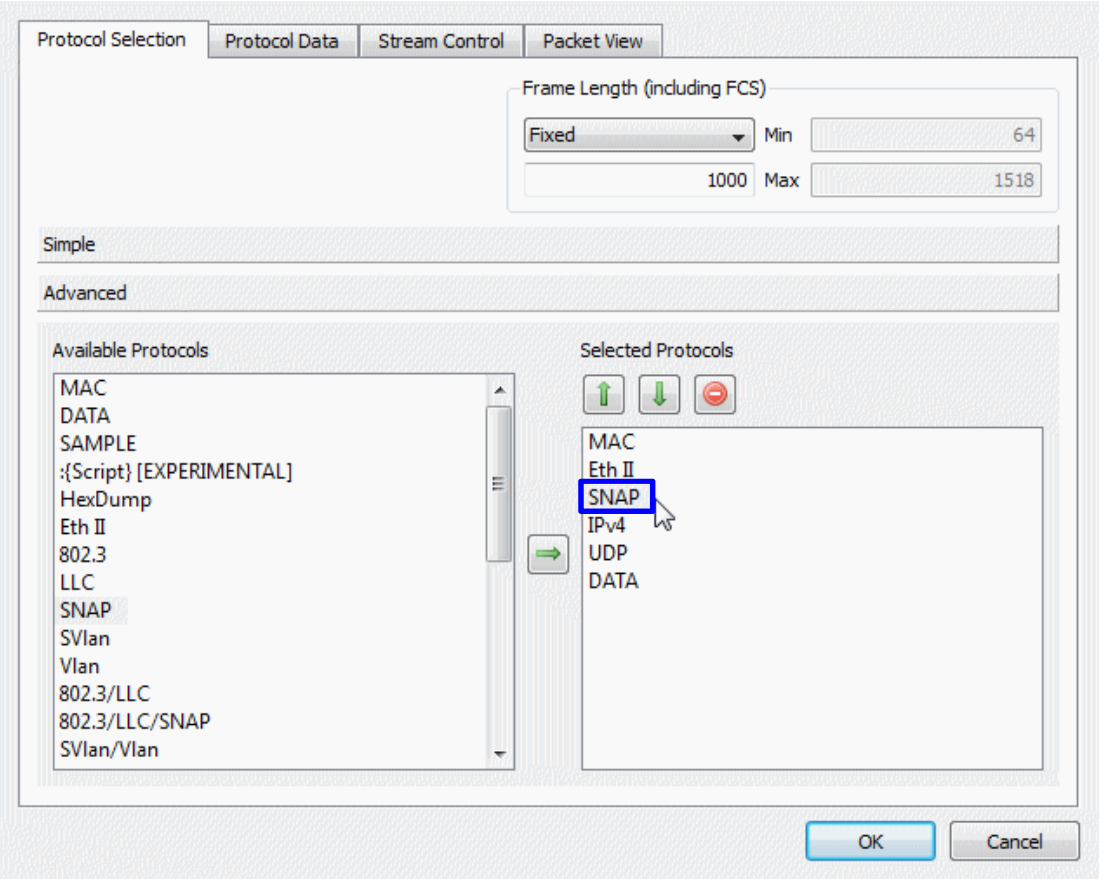


Figure-5: Add More Frame Fields if Required

Select the Protocol Data tab to enter the frame and packet data. In the Media Access Control section, enter the source and destination MAC addresses for the stream and choose whether you wish the MAC addresses to remain fixed or to increment or decrement. In this example I am using fixed MAC addresses.

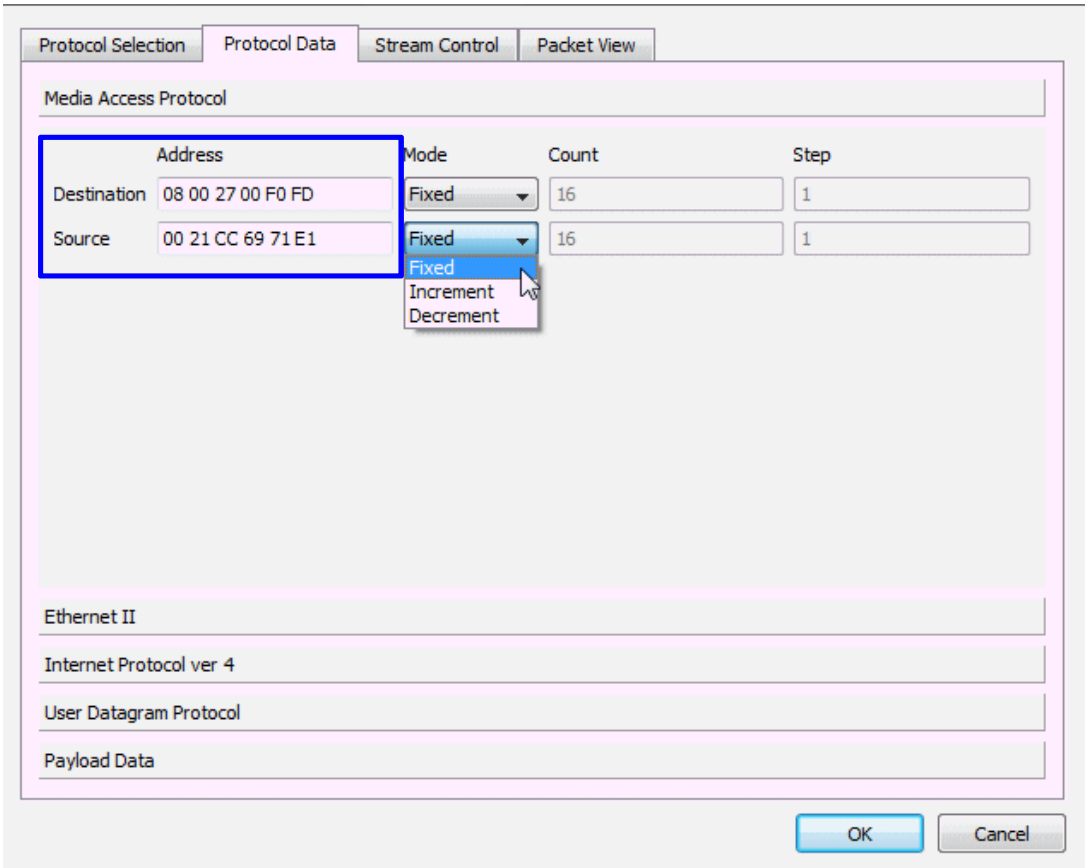


Figure-6: Frame and Packet Information

Select the Ethernet II section. Enter the Ethernet type. Tick the Ethernet Type box to change the default from 08 00 if desired.

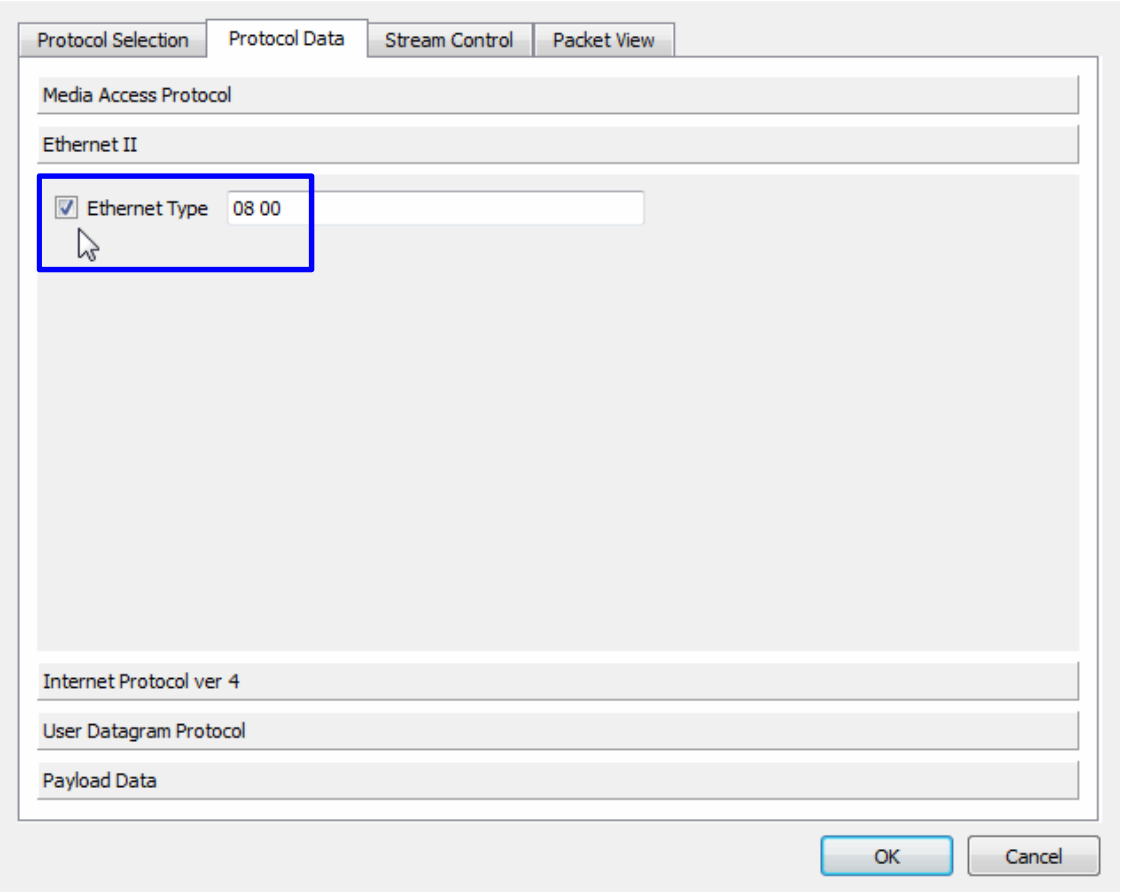


Figure-7: Ethernet Type

Select the Internet Protocol Version 4 section. Enter the required ToS/DSCP value from Table-2 above, the source and destination IP addresses and, if desired, choose whether to use fixed, incrementing or decrementing IP addresses.

In this example I am using Ostinato ToS/DSCP value B8 = decimal 184 = 10111000 binary. Taking the left-most six bits 101110 this equates to class selector 5 (101), and drop probability high (11), which is EF.

If desired, you can also change the following IPv4 parameters:

- Version
- Header length
- Total length of the datagram
- fragment ID number (default 04D2 = 1234)
- Fragment offset
- Don't fragment bit
- Passenger protocol number
- Checksum

It is advisable to leave the Override Checksum un-ticked as the software will generate a suitable value based on the information entered.

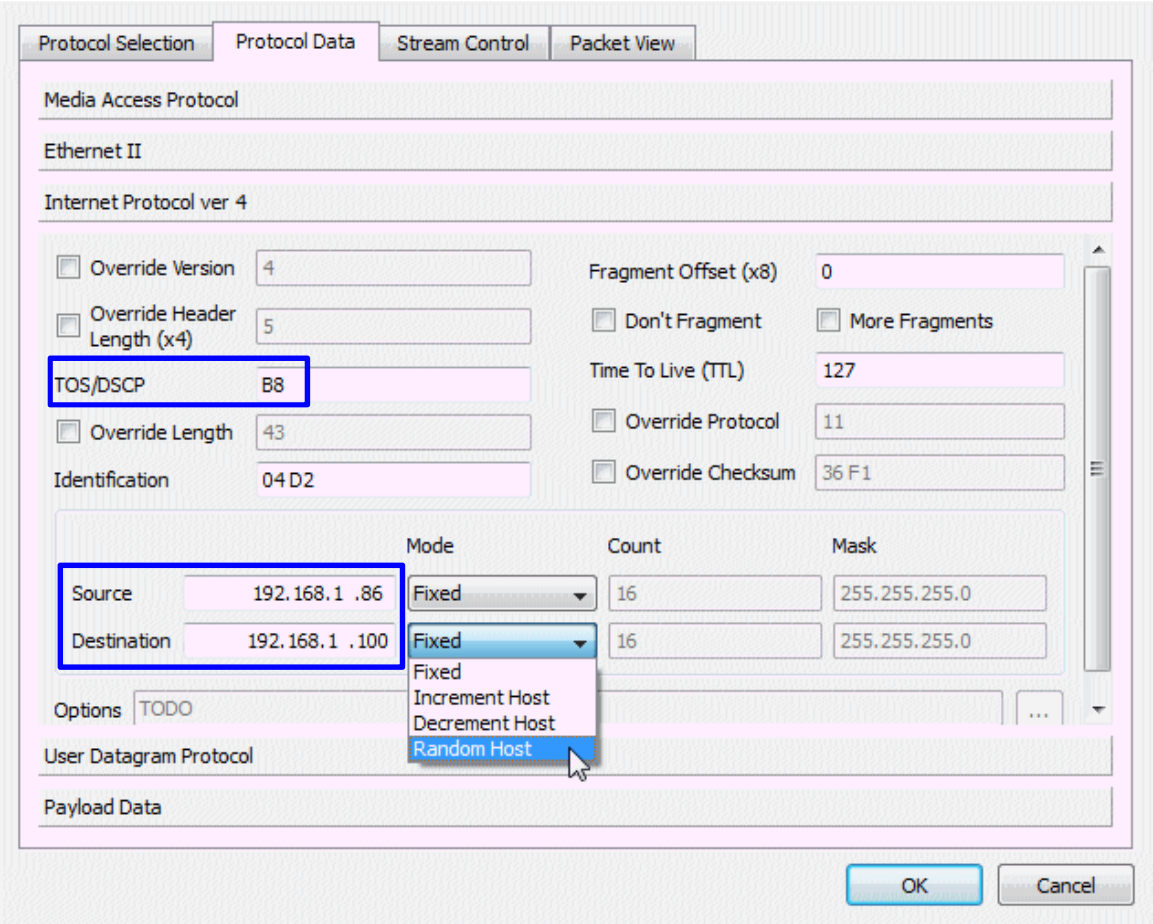


Figure-8: IPv4 Information

Select the User Datagram Protocol section if you wish to modify any UDP information. In this example I am using UDP source port 5000 and destination port 5001.

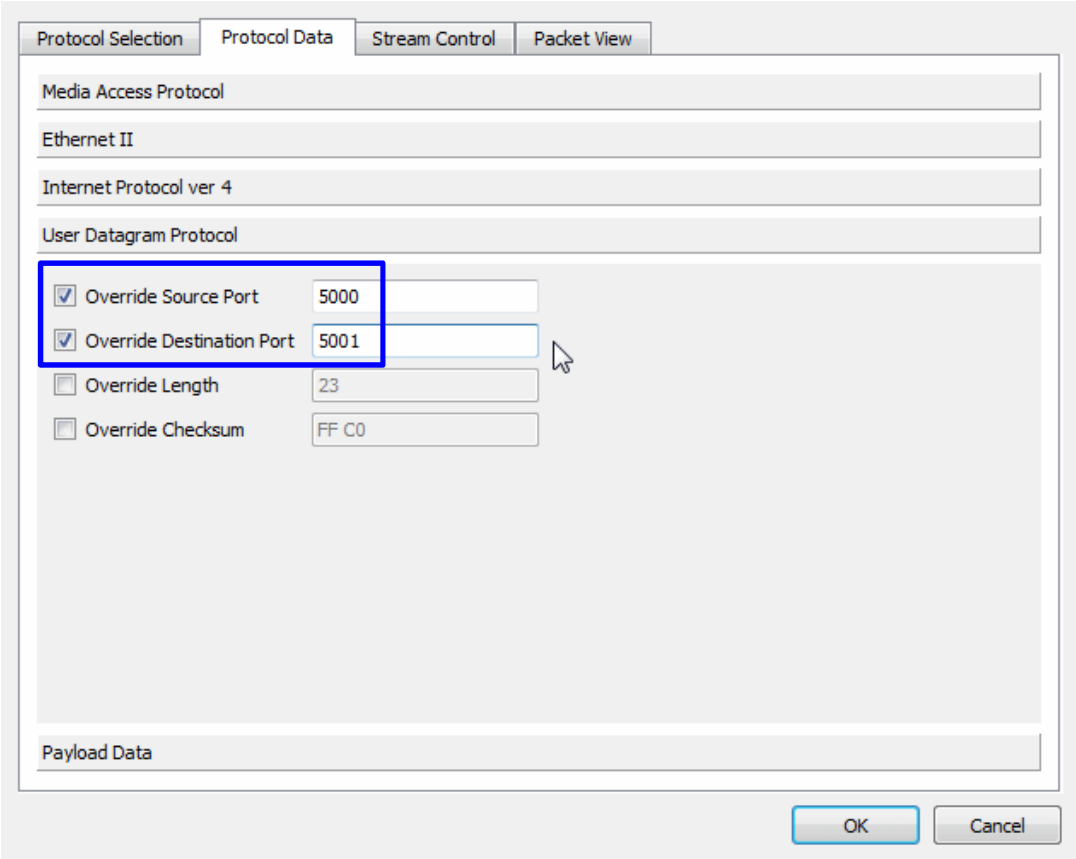


Figure-9: UDP Information

Select the Payload Data section if you wish to change the UDP payload data using a fixed, incrementing, decrementing or random pattern. This is useful if you wish to identify clearly the data that you are transmitting in packet captures.

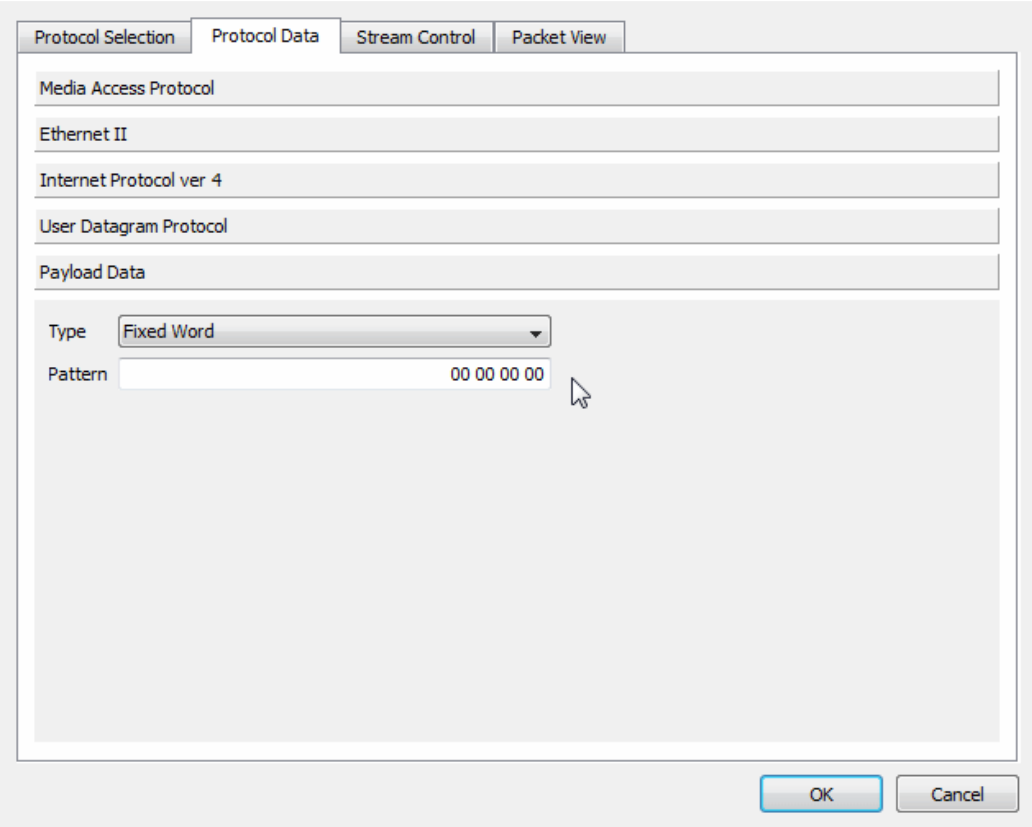


Figure-10: Payload Data

Select the Stream Control tab to configure the volume of traffic you wish to generate and the way in which the stream will behave.

In this example I am sending 10 packets at 1G per second. However, when transmission completes the Goto First radio button will cause the stream to loop endlessly. I could have configured a large number of packets in this stream and chosen to jump to the next stream, if I had more than one stream configured.

When configuring bits per second, the packets per second field adjusts automatically. When configuring the packets per second value, the bits per second value adjusts automatically.

It is also possible to select bursts of traffic and to specify how many bursts to transmit and the number of packets within each burst.

The values for ISG, IPG and IBG adjust automatically. These abbreviations are:

- ISG – Inter-Stream Gap
- IPG – Inter-Packet Gap
- IBG – Inter-Block Gap

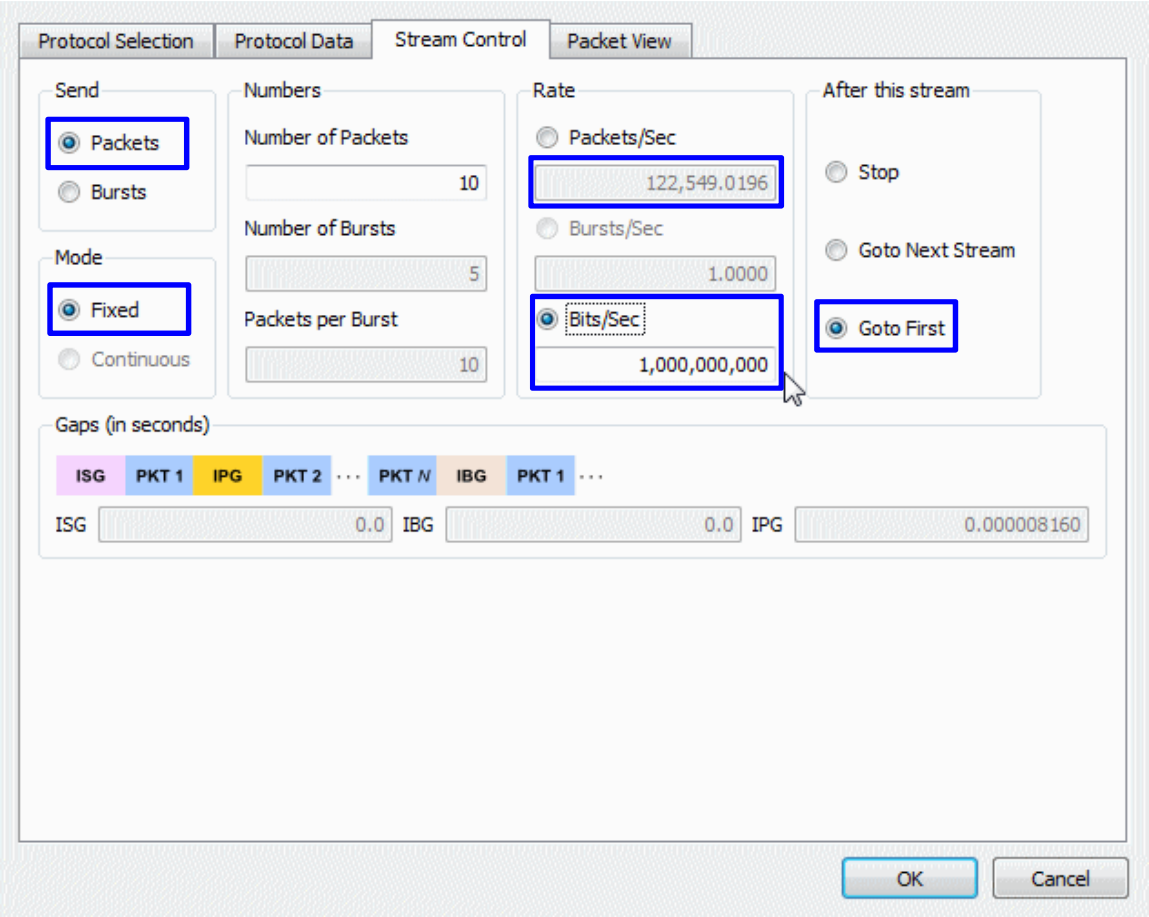


Figure-11: Stream Control

Select the Packet View tab to see a summary of the packets being generated. Click OK to complete the packet creation process.

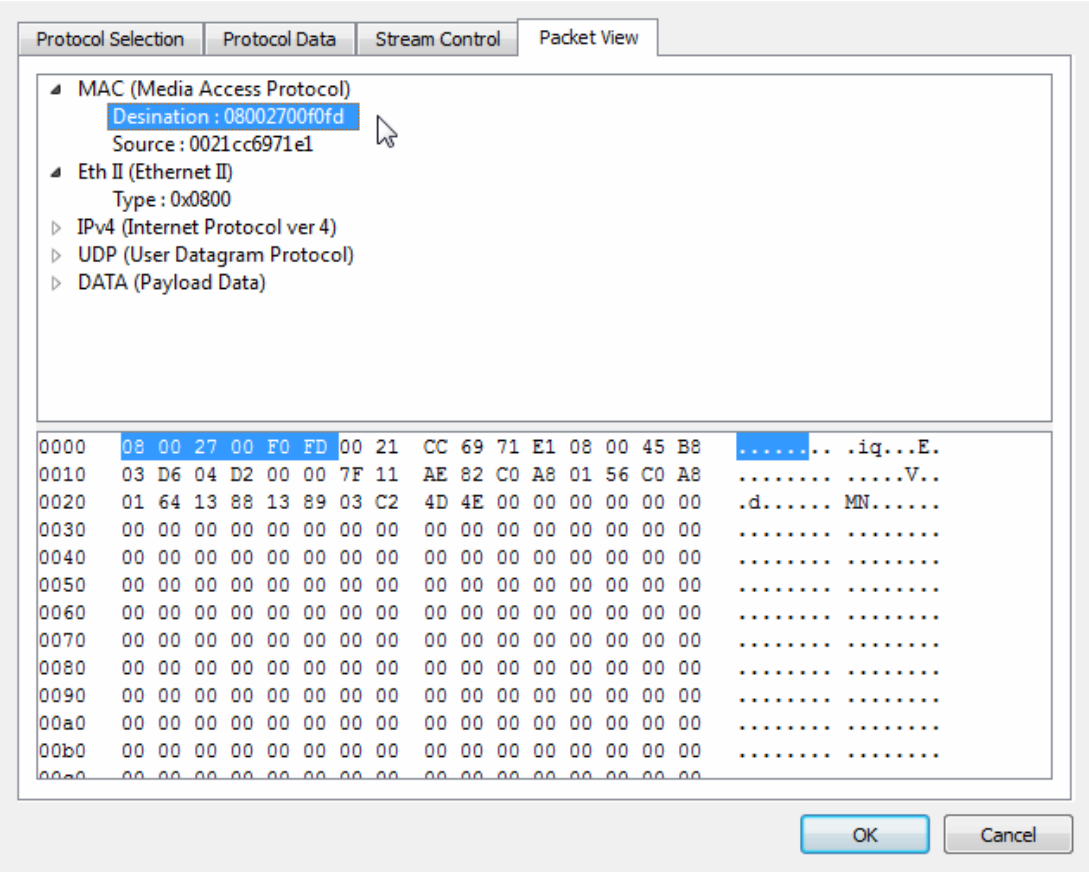


Figure-12: Packet Data Summary

3.3 Starting Streams

After creating the stream and clicking OK you are returned to the main Ports and Streams window.

Be sure to click Apply otherwise your changes will not take effect.

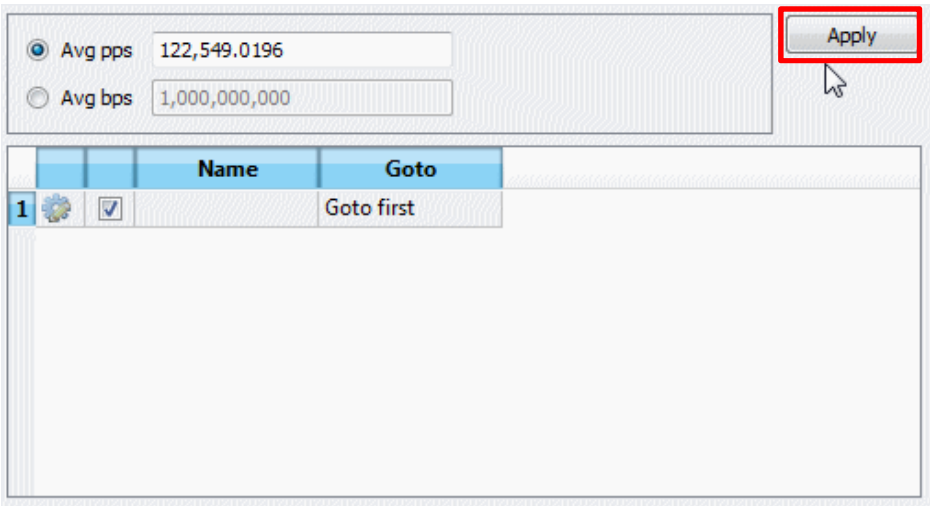
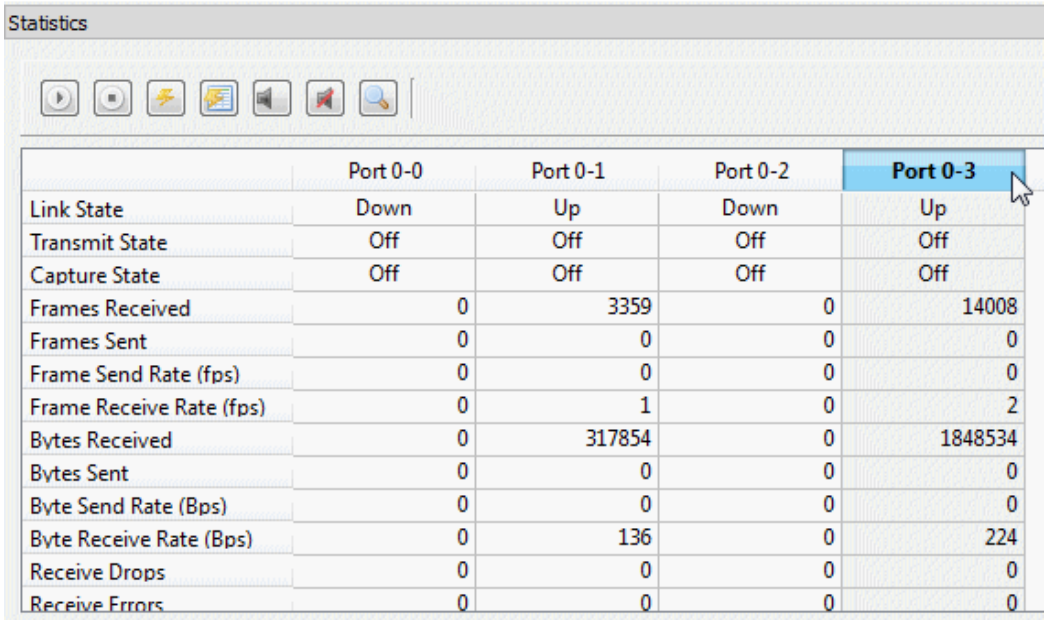


Figure-13: Apply Changes

The average packets and bits per second of your stream are displayed at the top of the streams pane.

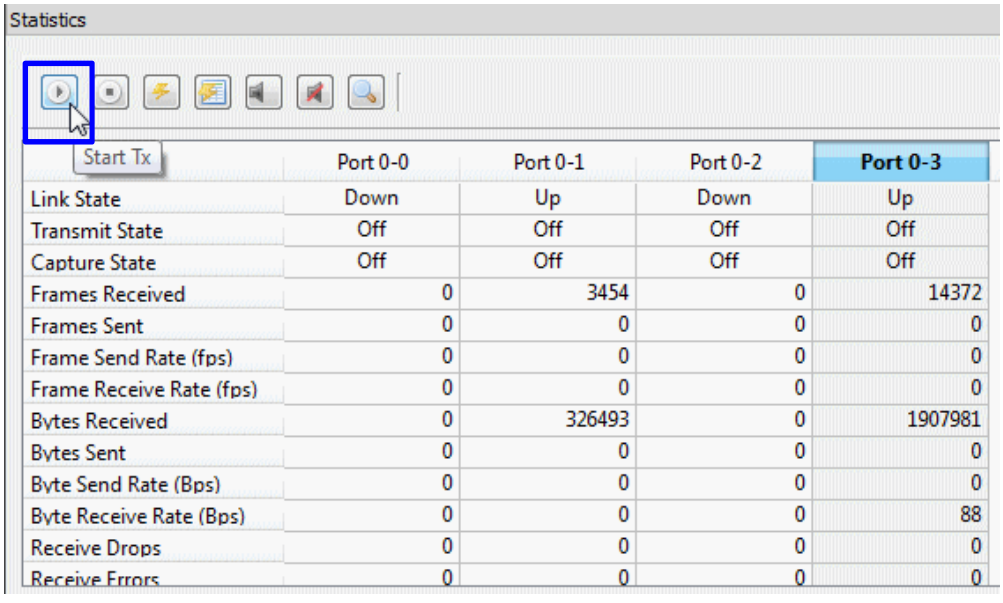
In the Statistics pane at the bottom of the main window, select the interface over which you wish to transmit the stream you have just created.



	Port 0-0	Port 0-1	Port 0-2	Port 0-3
Link State	Down	Up	Down	Up
Transmit State	Off	Off	Off	Off
Capture State	Off	Off	Off	Off
Frames Received	0	3359	0	14008
Frames Sent	0	0	0	0
Frame Send Rate (fps)	0	0	0	0
Frame Receive Rate (fps)	0	1	0	2
Bytes Received	0	317854	0	1848534
Bytes Sent	0	0	0	0
Byte Send Rate (Bps)	0	0	0	0
Byte Receive Rate (Bps)	0	136	0	224
Receive Drops	0	0	0	0
Receive Errors	0	0	0	0

Figure-14: Select the Stream Transmission Interface

Click the play button to start the stream. The statistics counters increment as the stream is transmitted.



	Port 0-0	Port 0-1	Port 0-2	Port 0-3
Link State	Down	Up	Down	Up
Transmit State	Off	Off	Off	Off
Capture State	Off	Off	Off	Off
Frames Received	0	3454	0	14372
Frames Sent	0	0	0	0
Frame Send Rate (fps)	0	0	0	0
Frame Receive Rate (fps)	0	0	0	0
Bytes Received	0	326493	0	1907981
Bytes Sent	0	0	0	0
Byte Send Rate (Bps)	0	0	0	0
Byte Receive Rate (Bps)	0	0	0	88
Receive Drops	0	0	0	0
Receive Errors	0	0	0	0

Figure-15: Start the Stream

The buttons to the right of the play button are:

- Stop stream

- Clear statistics of the selected port
- Clear statistics of all ports
- Capture packets on the selected port (starts Wireshark)
- End the packet capture
- View captured packets

3.4 Verifying Stream Packets

Initiate a packet capture from within Ostinato or start Wireshark on your laptop. Examine the packets to confirm that the stream settings are correct.

The packets are generated very rapidly according to the rate you have configured.

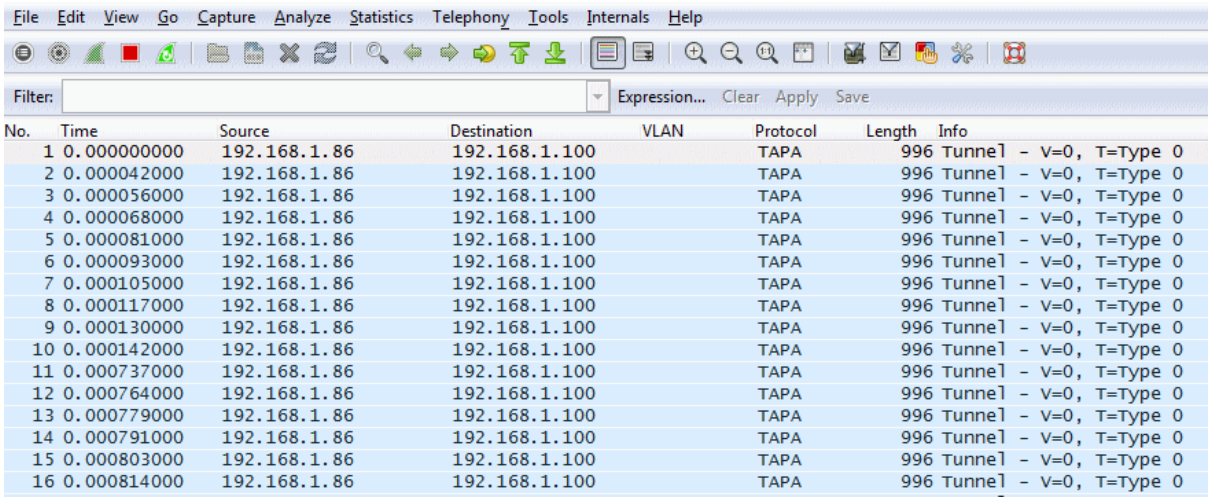


Figure-16: Verifying Stream Packets

Verify that the packet content is according to the stream configuration. The L2, L3 and L4 information is as configured. The 8-bit DSCP byte has value B8, including the 2 x ECN bits, and the 6 x DSCP bits have value $2E_{16} = 46_{10} = 101\ 110_2$.

The DSCP value is class 5 with drop probability high, which is EF.

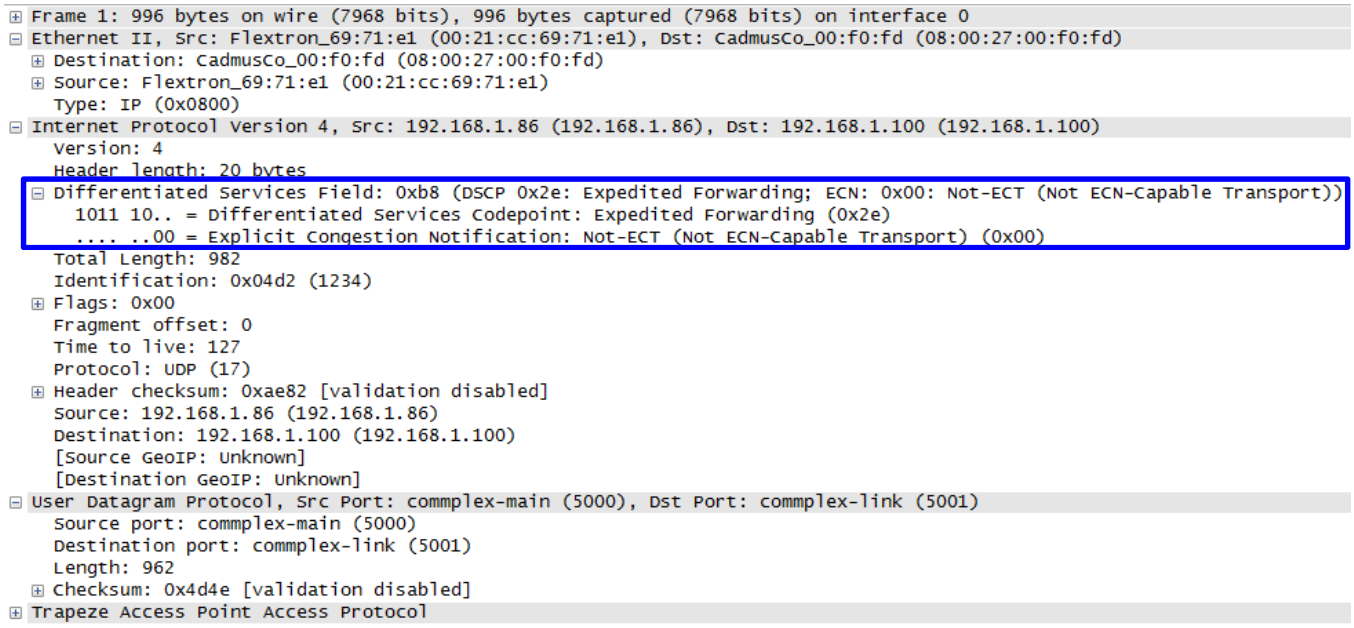


Figure-17: Verifying Packet Content