

NuDOG-301 DApps-SG Utility User Manual

USM: V1.0



Xtramus Technologies E-mail: sales@xtramus.com Website: www.xtramus.com Tel: +886-2-8227-6611 Fax: +886-2-8227-6622

Copyright

Copyright © 2008 Xtramus Technologies. All Rights Reserved. The information contained in this document is the property of Xtramus Technologies. No part of this publication may be reproduced, stored in a retrieval system, or transmitted, in any form or by any means, without the prior written permission of Xtramus Technologies.

Disclaimer

The information contained in this document is subject to change without notice and does not represent a commitment on the part of Xtramus Technologies. The information in this document is believed to be accurate and reliable, however, Xtramus Technologies assumes no responsibility or liability for any errors or inaccuracies that may appear in the document.

Trademarks

NuStreams is a trademark or registered trademark of Xtramus Technologies. All other trademarks and registered trademarks are the property of their respective owners.

Warranty

Xtramus Technologies warrants to recipient that hardware supplied with this document will be free from significant defects for a period of three (3) months from the date of delivery, under normal use and conditions. Defective Product under warranty shall be, at Xtramus Technologies' discretion, repaired or replaced. To the extent permitted by applicable law, all implied warranties, including but not limited to imply warranties of merchantability, non-infringement and fitness for a particular purpose, are hereby excluded, and the liability to Xtramus Technologies, if any, for damages relating to any allegedly defective product shall be limited to the actual price paid by the purchaser for such product. In no event will Xtramus Technologies be liable for costs of procurement of substitute products or services, lost profits, or any special, direct, indirect, consequential, or incidental damages, however caused and on any theory of liability, arising in any way out of the sale and/or license of products or services to recipient even if advised of the possibility of such damages and notwithstanding any failure of essential purpose of any limited remedy.



REVISION HISTORY

Date	FW Version	FPGA Version	USM Version	History
August, 2009			1.0	First draft version



Table of Contents

Table of	Contents	3
1. Gen	eral Description	6
1.1 F	eatures	6
1.2 F	unction Mode	7
1.2.1	Stream Generation Mode	7
1.2.2	TAP mode	7
1.3 S	upport Software	8
1.3.1	DApps-SG: Control Suite for Multiple Streams Generator	8
1.3.2	DApps-TAP: Ethernet TAP Suite base on TAP and Loopback	8
1.3.3	DApps-NIC: Network Card Simulation Suite	8
1.3.4	DApps-2544: Test Suit Based on RFC-2544	8
1.3.5	DApps-2889: Test Suit Based on RFC-2889	8
1.3.6	DApps-MPT: Automated Batch Tests for Ethernet Device	9
1.3.7	DApps-QoS: QoS Testing based on VLAN items	9
1.3.8	DApps-QoS3: QoS Testing Based on IP/UDP items of Layer3	9
1.3.9	DApps-RGW: Test for Router Gateway	
2. App	earance	10
2.1 L	eft Side	10
2.2 To	op side	10
2.3 R	ight side	12
3. DAp	ps-SG Stream Generation Utility	14
3.1 Ir	stallation of Software Utility	14
3.2 O	peration Menu	
3.2.1	File Sub-menu	
3.2.2	Statistics Sub-menu	
3.2.3	Control Sub-menu	
3.2.4	Service Sub-menu	
3.2.5	Help Sub-menu	
3.3 To	oolbar	19
3.4 C	onfiguration and Information Zone	22
3.4.1	System Information	
3.4.2	Port Status and Configuration	23
	3.4.2.1 Media Config	23



		3.4.2.2 Media Status	23
		3.4.2.3 Multi Streams Generation	24
		3.4.2.4 Capture Criteria	27
		3.4.2.5 Capture Buffer	
	3.4.3	Control Panel	
	3.4.4	Report	
		3.4.4.1 VLAN Stream Counter Window	34
		3.4.4.2 X-TAG Stream Counter Windows	35
	3.4.5	Function	
		3.4.5.1 DUT-Clock	37
	3.5 Fr	ame Editor	
	3.5.1	Overview	
		3.5.1.1 Import	40
	3.5.2	Frame View	
	3.5.3	Data Link layer	41
		3.5.3.1 Ethernet II	41
		3.5.3.2 Variation of DA, SA and VID	42
		3.5.3.3 IPX	43
	3.5.4	Tags	43
		3.5.4.1 VLAN	43
		3.5.4.2 Q-in-Q	44
		3.5.4.3 MPLS	45
	3.5.5	Layer 3 Header	47
		3.5.5.1 IPv4	47
		3.5.5.2 ARP	49
		3.5.5.3 Pause	50
	3.5.6	Layer 4 Header	
		3.5.6.1 TCP/IP	51
		3.5.6.2 UDP/IP	
		3.5.6.3 ICMP/IP	53
		3.5.6.4 IGMP/IP	54
4.	Oper	ation of NuDOG-301 with DApps-SG	56
	4 1 Cr	ontrol from LISB Port	56
	411	Installation of Driver	
	4.2 Ha	ardware connection	57
	4.3 Op	peration of DApps-SG	
	4.3.1	Generate Test Streams to DUT	57
		4.3.1.1 Start to generate test streams	59



4.3.2	Capture Specified Packets	59
4.3.3	View counter of captured packet and others	61



1. General Description

NuDOG-301 is a two ports handheld network TAP and streams generating equipment. Innovative design makes it unique from other test equipment. Unlike other network TAP equipment, NuDOG-301 has USB port for both system configuration / management and network TAP. For TAP function, streams flow through NuDOG-301 is tapped and forwarded to PC via USB. Advanced criteria can filter the packet wanted to reduce the traffic to PC dramatically.



In addition to the passive mechanism, NuDOG-301 is also an active stream generator that can generate test streams with variety of Ethernet frames and test protocols. Two ports of NuDOG-301 can work as pair to have Rapid-Matrix stream test for the DUT. BERT pattern loopback test can find the errors due to the DUT.

For network test equipment with such capability and availability, NuDOG-301 indeed reduces the research and development lead-time, do great help to find the faulty product by batch network test and also get the way to find the possible bottleneck of the network for MIS in office. Elegant hairline surface coating outside and excellent feature inside make NuDOG-301 the best choice of handheld network test device.

1.1 Features

- 10/100/1000 Mbps Wirespeed Stream generation, TAP, capture, and analysis
- Rapid-Matrix multi-streams generation for simultaneous network test
- Proprietary X-TAG frame tagging technique for examination of latency, packet loss, and packet sequence...etc.
- SDFR technique make capture of Ethernet frame easy and convenient
- Stream Counter per port for detailed analysis of test result
- Pre-defined or user-defined patterns as trigger conditions of Multi-stream Counter
- Active TAP feature that analyze and filter all packets flows through without interfering the original traffic
- Uni-directional streams between bi-directional network traffic can be redirected to PC for analysis
- Complete real-time RMON counter for analysis
- Layer 1 and Layer 2 passive loopback mode for incoming traffic
- Supports 2 ports Cross-loopback or one port Local-loopback
- Verify oscillator's speed rate of DUT



• Variety of application software for different test requirement

1.2 Function Mode

1.2.1 Stream Generation Mode

For Streams Generation mode, the NuDOG-301 generates bi-directional network streams for required test as the illustration below.

Both Port A and Port B of NuDOG-301 can generate and receive test streams. The test streams are sent and return to original NuDOG-301 for analysis of the DUT (device under test).



1.2.2 TAP mode

For TAP mode, NuDOG-301 can monitor any data that flows through this equipment. Network TAP is the way to monitor running network without intruding the network. NuDOG-301 can tap bi-directional or uni-directional traffic from different sides and also provides abundant packet counters





1.3 Support Software

There are several software that can work with NuDOG-301 for different kind of test requirement. Here is the introduction of these software. Please contact with distributor to purchase suitable utility software for your test.

1.3.1 DApps-SG: Control Suite for Multiple Streams Generator

Please read the following chapter to know how to operate this software. DApps-SG provides a powerful and sophisticated virtual front control panel to manage the NuDOG-301. Two test ports can be independently configured with parameters to define multiple streams, filters, and capture capabilities. Traffic for various network protocols can be customized, transmitted, and received on each port. Comprehensive statistics provide users an in-depth analysis of the performance of the DUT (Device Under Test).

1.3.2 DApps-TAP: Ethernet TAP Suite base on TAP and Loopback

For NuDOG-301, all data streams between two network ports can be duplicated and sent to PC via USB port for monitor and analysis. Operator can specify criteria to filter the packets wanted by DApps-TAP application software. It reduces the network traffic of USB port and also decreases the resource of PC to deal with large quantity of packets.

*In theory, maximum speed of USB 2.0 is 480Mbps and maximum speed of UTP port is 1GMbps. For data transmission over 480Mbps, the packets to USB port are dropped if all packets are tapped by USB port. However, it does not affect the data transmission flows between two network ports.

1.3.3 DApps-NIC: Network Card Simulation Suite

NuDOG-301 has a mini-USB port for connection to PC. In addition to network TAP, system control and system upgrade of NuDOG-301, it also has the function of network interface card. By the software control and hardware conversion of NuDOG-301, network data streams can flow between USB and network port of NuDOG-301.

*In theory, maximum speed of USB 2.0 is 480Mbps and maximum speed of UTP port is 1GMbps. Enable flow control can prevent packet loss if the network transmission is over 480Mbps

1.3.4 DApps-2544: Test Suit Based on RFC-2544

DApps-2544 is a user-friendly and automated test suite based on industry-standard RFC-2544. It generates and analyzes the packets to evaluate the performances of Throughput, Latency, Packet Loss, and Back-to-Back of Ethernet switches or routers via NuDOG-301. The real-time display of test results and customized report provide an effective way to examine the DUT.

1.3.5 DApps-2889: Test Suit Based on RFC-2889

DApps-2889 is a user-friendly and automated test suite based on industry-standard RFC-2889 to test the DUT. RFC 2889 provides methodology for the benchmarking of local area network (LAN)

XTRAMUS TECHNOLOGIES[®]



switching devices, forwarding performance, congestion control, latency, address handling and filtering. It extends the methodology already defined for benchmarking network interconnecting devices in RFC 2544.

1.3.6 DApps-MPT: Automated Batch Tests for Ethernet Device

DApps-MPT is an accurate and efficient software suite for mass production test or batch network test. Various packet generation and reception testing items could be configured to pre-defined testing modes. The utility of DApps-MPT is easy to load testing models. All simple and visualized results and detailed testing logs are available to be accessed based on requirements. DApps-MPT is a powerful and convenient tool to apply on NuDOG-301.

1.3.7 DApps-QoS: QoS Testing based on VLAN items

Network QoS (quality of service) is a way to classify the transmission priority of packets when the packets that are going to transmit are beyond the throughput that the Ethernet switch or router is able to deal with. Higher priority packets are processed and transmitted first.

For Ethernet frame, each packets can be tagged with a VLAN ID and CoS (class of service). For Ethernet switch or router that supports QoS, packets with higher CoS priority should be transmitted first if traffic is congested. DApps-QoS is able to limit acceptable network traffic at receiving port and analyze the traffic distribution of packets with different priority received from DUT (router or switch).

1.3.8 DApps-QoS3: QoS Testing Based on IP/UDP items of Layer3

The QoS (quality of service) of DApps-QoS3 is similar to DApps-QoS. Layer 3 IP/UDP packets are marked according to the type of service they need. In response to these markings, routers and switches use various queuing strategies to tailor performance to requirements. By the same test mechanism, NuDOG-301 tests the performance of Layer 3 Router, Switch with QoS function.

1.3.9 DApps-RGW: Test for Router Gateway

DApps-RGW is an application software to test the router/ gateway. By this application, NuDOG-301 simulates as a DHCP clients that request service or generate streams to test the performance of the router/gateway. The volume of allowable DHCP clients, PPPoE authentication, throughput, latency, QoS, sessions allowed and protocols such as FTP, UDP and TCP can be tested or measured.



2. Appearance

2.1 Left Side

There are holes with fan for ventilation



Connection Ports

Port Type	Label	Description
USB Port		Management, configuration or firmware/FPGA update of this machine.
		For TAP mode, it also re-directs tapped packets to PC.
Power Jack	12V DC	Plug power from DC 12V adapter
	$\ominus - \ominus - \ominus$	
FAN		Fan hole with internal fan for ventilation.
Diagnostic Port	Diagnostic	Optional diagnostic port (reserved)

2.2 Top side

Indication LEDs are all located here.





LED Status

Туре	Label	LED	Description
Power	Power Fail	Green	Power is ON without problem
		Yellow	System is failed
		(Amber)	
Port Status	USB	Green	USB of this device is linked to PC
		Yellow	No USB link
		(Amber)	
Operation Mode	SG TAP	Green	Stream generation mode is activated.
			When it works with the utility software
			below. LED is green.
			• DApps-SG
			• DApps-2544
			• DApps-2889
			DApps-MTP
			 DApps-QoS
			DApps-QoS3
		Yellow	TAP mode is activated. TAP is the
		(Amber)	method to monitor network traffic that
			flows through this device. When it
			works with DApps-TAP utility software,
			the LED is Yellow
		OFF	When it works DApps-NIC, the LED is
			off.



Capture Port	Capture A	Green	Capture Mode of A port is activated
	Capture B	Green	Capture Mode of B port is activated

2.3 Right side

Right side has ports that connect with physical transmission media.



Connection Ports

	Port Type	Label	Description	
А	SFP port	A	SFP port for 1G speed SFP fiber connector	Only one port can be used
	Ethernet port for RJ-45 connector		Ethernet port for 10/100/1000M speed connection of RJ-45 connector	simultaneously
В	Ethernet port for RJ-45 connector	В	SFP port for 1G speed SFP fiber connector	Only one port can be used
	SFP port		Ethernet port for 10/100/1000M speed connection of RJ-45 connector	simultaneously



LED Status

Туре	Label	LED	Description
UTP Port status for	Link/ACT	ON	Network is linked
RJ-45 connector		Blinking	Data is transmitting or receiving
	Speed	ON	1000Mbps connection
		Blinking	100Mbps connection
		OFF	10Mbps connection if Link/ACT is ON
			or blinking



3. DApps-SG Stream Generation Utility

DApps-SG provides a powerful and sophisticated virtual front control panel to manage the NuDOG-301. Two test ports can be independently configured with parameters to define multiple streams, filters, and capture capabilities. Traffic for various network protocols can be customized, transmitted, and received on each port. Comprehensive statistics provide users an in-depth analysis of the performance of the DUT (Device Under Test).

3.1 Installation of Software Utility

Click to run the .EXE utility execution file provided by Xtramus to install the software. System shows





Image: Customer Information Image: Customer Information Please enter your information. Image: Customer	Input User Name and Organization and click Anyone who uses this computer (all users) and Next
Organization:	
< <u>Back</u> <u>N</u> ext > Cancel	
Image: Section program features will be installed. (Requires the most disk space.)	Select Complete setup type, and then click Next. If you want to install the utility other then default directory, then select Custom .
Choose which program features you want installed and where they will be installed. Recommended for advanced users. InstallShield < Back Next > Cancel	
🔁 DApps-SG - InstallShield Wizard	The message prompt you that
Ready to Install the Program The wizard is ready to begin installation.	installation is going to start. Click Next to
Click Install to begin the installation. If you want to review or change any of your installation settings, click Back. Click Cancel to exit the wizard. InstallShield	continue.
< <u>Back</u> Install Cancel	



Microsoft Visual C++ 2005 SP1 Redistributable Package (x86)	The system prompts you that installation
Please read the following license agreement. Press the PAGE DOWN key to see the rest of the agreement.	of Microsoft Visual C++ SP1
MICROSOFT SOFTWARE LICENSE TERMS MICROSOFT VISUAL C++ 2005 RUNTIME LIBRARIES These license terms are an agreement between Microsoft Corporation (or based on where you live, one of its affiliates) and you. Please read them. They apply to the software named above, which includes the media on which you received it, if any. The terms also apply to any Microsoft * updates, * supplements, * supplements, * Internet-based services, and * support services for this software, unless other terms accompany those items. If so, those terms apply. By using the software, you accept these terms. If you do not accept Do you accept all of the terms of the preceding License Agreement? If you choose No, Install will close. To install you must accept this agreement.	Redistributable Package is required. Click Yes to install it and the installation is started.
DAppeSG - InstallShield Wizard InstallShield Wizard Completed The InstallShield Wizard has successfully installed DApps-SG v0.9b002. Click Finish to exit the wizard.	Click Finish to close the installation procedure

When Installation is done, start the program by clicking Start \rightarrow All Programs \rightarrow Xtramus \rightarrow



DApps-SG vx.xxxxx ("x" is version number) or vx.xxxxx at desktop, then main windows is shown.

3.2 Operation Menu

The operation menu is located at top of this utility





3.2.1 File Sub-menu

Block in main window: A

The second se
 Report resources

File Statistics Co.	
Exit Ctrl+Q	
Menu Choice	Usage
Exit	Exit and close this utility

3.2.2 Statistics Sub-menu





Menu Choice	Usage
Control Panel	Real-time frame counters and control panel of Port A and Port B. The counters contain frame counts generated and received that can
	examine the DUT.
VLAN Stream	Add VID (VLAN ID) in specified range into the Ethernet frames that is
Counters Window	generated from port A and/or port B in order to test DUT that supports
	VLAN tagged frame.
	Complete VLAN stream counter can analyze the packet sent and
	received.
X-TAG Stream	X-TAG is an Xtramus proprietary 12 bytes embedded tag that is
Counter Window	located at 49th~60th bytes of each testing frames that are generated
	by Rapid-Matrix for multi-streams tests.
	This counter can analyze many detailed problems of network
	transmission of Port A, Port B and Port A+B. They contain counters
	Current Tx Rate, Packets, Bytes, Loss Packets, S/N (serial number)
	Miss and IPCS (IP Checksum) Error.
Port A Stream	Configure the settings and contents of port A for the generation of
Gen	packet streams
Port A Stream	Configure the settings and contents of port B for the generation of
Gen	packet streams

3.2.3 Control Sub-menu

File	Statist	ics	Cont	rol	Serive	s I	He	lp	
	5		Ca		re Buffe	er	۶	¥	Standard Mode (2K Size)
Recor	nent	Ca	ntiols	VL	AN SC	Х-	T7		Jumbo Mode (16K Size)

Menu Choice	Usage
Capture Buffer	Standard Mode (2K size): Active capture buffer (built-in memory) mode for maximum 2K size packets
	Jumbo Mode (16K size): Active capture buffer (built-in memory) mode for maximum 16K size packets



3.2.4 Service Sub-menu

File Statistics Control	Serives Help
Reconnent Controls VI	System Upgrade FPGA Upgrade
Information	Log Window Ctrl+L

Menu Choice	Usage
System Upgrade	Do system upgrade for
	Firmware: Firmware in this machine
FPGA Upgrade	Do system upgrade for
	FPGA: (Field Programmable Gate Array) chip in this machine
Log Windows	See instant log of current running command and result

3.2.5 Help Sub-menu

File	Statistics	Control	Serives	Help
		₽		About NuDOG301

Menu Choice	Usage
About (Model	System information, such as Utility version and Hardware version of
Name)	this device
Xtramus Web	Connect to Xtramus Web directly.

3.3 Toolbar

The Toolbar is located below operation menu of this utility Block in main window: **B**



Carlotte Ca	D
All Accesses	
Municipal Action Municipality Sections Calify Office	DALLS-SG
- Ban Harris	agent these rate of Results rests; etc.
Birt of the State	
A CONTRACTOR	

Reconnent	Dentrols	VLAN SC	X-TAG SC	SG A	SG B	Cap,C A	Cap,C B
E	F	G	н	1	J	K	L

Keys	Usage				
Reconnect	For accident case such as power loss, cable disconnected that the network is disconnected, press this button to reconnect the network.				
Controls	Real-time frame counters and control panel of Port A and Port B. The counters contain frame counts generated and received that can examine the DUT. This button is the same as main operation menu below File Statistics Control Serives Help Control Panel VLAN Stream Counter Window X-TAG Stream Counter Window Port A Stream Gen Port B Stream Gen				
VLAN SC	 VLAN Stream Counters Add VID (VLAN ID) in specified range into Ethernet frame that is generated from port A and/or port B in order to test DUT that support VLAN tagged frame. Complete VLAN stream counter can analyze the packet sent and received. This button is the same as main operation menu below 				



	File Statistics Control Serives Help Control Panel Control Panel Record VLAN Stream Counter Window Info X-TAG Stream Counter Window Port A Stream Gen Port B Stream Gen Port B Stream Gen Externation
X-TAG SC	X-TAG is an Xtramus proprietary 12 bytes embedded tag that is
	located at 49th~60th bytes of each testing frames that are
	generated by Rapid-Matrix for multi-streams tests.
	This counter can analyze many detailed problems of network transmission of Port A, Port B and Port A+B.
	This button is the same as main operation menu below
	File Statistics Control Serives Help Control Panel Control Panel VLAN Stream Counter Window Info X-TAG Stream Counter Window Port A Stream Gen Port B Stream Gen
SG A	Configure the settings and contents of port A for the generation of
	packet streams
	This button is the same as main operation menu below
	File Statistics Control Serives Help Control Panel Control Panel VLAN Stream Counter Window Info X-TAG Stream Counter Window Port A Stream Gen Port B Stream Gen
SG B	Configure the settings and contents of port B for the generation of
	packet streams
	File Statistics Control Serives Help Control Panel Control Panel VLAN Stream Counter Window Info X-TAG Stream Counter Window Port A Stream Gen Port B Stream Gen
Cap, C A	Configure the criteria to capture the packets from port A.
Сар, С В	Configure the criteria to capture the packets from port B.



3.4 Configuration and Information Zone

Block in main window: C

the over soir that	B B DEMI
Constant of the second se	DA _{FFS} -SC

For different selections, there are System Information, Configuration and Status of Port A, Port B, Report and Function Configuration in this block.

3.4.1 System Information

Click the item below to show the system information

Information						
🕦 S/N : 0JDOG30000XX						
1 MAC : 00-22-A2-22-XX-XX						

On the right side of the main window, it shows

Model	NuDOG-100/301
Agent	Agent/Customer
s/N	0JDOG30000XX
MAC	00-22-A2-22-XX-XX
Hardware Version	v.MP05
API Version	v1.0b000
FPGA Version	v1.0b000
Manufacture Date	2009/08/12
Туре	DEMO

XTRAMUS TECHNOLOGIES[®]



3.4.2 Port Status and Configuration

Click the item of ports to show the status or configuration



3.4.2.1 Media Config

Click item below to configure the link mode. Port A and port B has the same configuration items

-------Boot A -------Media Config : Auto 1000M Full

User can view the media link status or force to run specified media link

Port A : Media Configuration

Auto	Force
O 10M Half duplex	C Force 10M Half duplex
O 10M Full duplex	C Force 10M Full duplex
O 100M Half duplex	C Force 100M Half duplex
O 100M Full duplex	O Force 100M Full duplex
1000M Full duplex	O Force 1000M Full duplex
	O Disable
	Apply cancel
Click Apply to take effect the configu	uration on this page or click cancel to resume

the original configuration

3.4.2.2 Media Status

Click items below to view the media status at its sub-tree.



— 🖃 Media Status	

Link : Link Up
16 Speed : 1000M Full

🗙 Type : Copper

This window shows current link and media status

Link Link Up Speed 1000M Full dulpex Mode 1000M Full dulpex Type Copper

3.4.2.3 Multi Streams Generation

Click item below to view the Multi Streams Generation configuration window.



The configuration is the same as selection in operation menu or toolbar as below

File	Statistics Control Serives Help	
	Control Panel	
Recon	VLAN Stream Counter Window	
Info	X-TAG Stream Counter Window	_
··· _ ··· <i>4</i>	Port A Stream Gen	8
6	Port B Stream Gen	or Toobar:

Operation Menu:

System shows the configuration window. User can configure the streams patterns for streams generation. Maximum 64 entries are allowed for this configuration.



Port A : Multi Streams Generation										
Save A										
Number of	Number of Streams 1									
Stream	# Select	Length	Rate	X-1	rag 🛛	Append	Frame Data	Protocol		
	Stream	(no CRC)	PPS -	En	X-ID	CRC	Config	Туре		
1	~	60	1000			~	Frame Edit	LLC		

Continued

J D	A	K s	A		(D	Μ	0	
Mode Range		Mode Range Mode Range		IFG	IBG	Frames		
Fixed		Fixed		Fixed		96	999327904	1000

- A: Save button: Save the configuration of current settings
- B: Number of Streams: Volume of streams that will be generated
- C: Select Stream □: User can tick the □ to active the stream generation of this stream.
- D: Length (no CRC): Frame length in bytes without CRC
- **E**: Rate: Select the unit and input the value of the parameter that the packets will be generated.
 - ✓ Packet per Second: PPS Utilization: % Line Rate: Mbps

PPS: Packet per second. Volume of packets that will be generated per second. Utilization: Percentage of Wirespeed transmission

Line Rate: Mbytes per second in transmission

F: X-TAG En \square : User can tick the \square to active tag generation of X-TAG. When it is ticked, user can select X-ID. Each X-TAG has an unique ID. If there are more than one product of Xtramus is generating the data stream on the same network, their X-ID should be different

X-TAG that is used as stream tags for providing fundamental information for collecting statistics of multi-stream traffic. Advanced tests like latency, packet loss, and packet sequence miss can be realized by X-TAG.

X-TAG is an Xtramus proprietary 12 bytes embedded tag that is located at 49th~60th bytes of each testing frames that are generated by Rapid-Matrix for multi-stream tests.



G: Append CRC: Add CRC checksum to the end of each frame. CRC checksum is the way to

XTRAMUS TECHNOLOGIES[®]



verify the correctness after data transmission. 4 bytes will be added at the end of the frame when CRC checksum is added.

H: Frame Data Config: Configure the payload contents in frame. Click the Frame Editor

Frame Editor to edit the detailed contents in frame. For the detail of how to use Frame Editor, please refer to 3.5 Frame Editor

I: Protocol Type: System shows the Protocol Type when frame content is configured in Frame Editor

J: DA: Mode: Show or configure current Destination Address Mode. It can be Fixed, Increase, Decrease or Random. If increase or decrease mode is selected, configure range (0~255) is required. The DA will increase or decrease according to the range and repeat again. For the detail of this function, please refer to 3.5 Frame Editor

K: SA: Mode: Show or configure Source Address Mode. It can be Fixed, Increase, Decrease or Random. If increase or decrease mode is selected, configure range (0~255) is required. The SA will increase or decrease according to the range and repeat again. For the detail of this function, please refer to 3.5 Frame Editor

L: VID: Mode: Show or configure VID Mode. It can be Fixed, Increase, Decrease or Random. If increase or decrease mode is selected, configure range (0~4095) is required. The SA will increase or decrease according to the range and repeat again. For the detail of this function, please refer to 3.5 Frame Editor

Summary: The summary of the stream that user create

M: IFG: Interframe Gap. Ethernet devices must allow a minimum idle period between transmissions of Ethernet frames. It is called interframe gap (IFG) as the illustration below

Frame IFG Next Frame

The minimum interframe gap is 96 bits time or 12 byte time. It is the time taken for transmission of 96 bits raw data on the media.

N: IBG: Inter Burst Gap. Gap between each burst streams.

O: Frames: Total frames that will be sent



Port A : 7	Madiki Sele	uana Ge	enele					
르								
NAME OF TAXABLE	98.F		2048-00	NI MIL	100 J	ънста 🖓	- m	
Street P	Salari.	Longitz		dan k	e00	S Argent 1	in analysis	Protocol
	- 61	den surelli	100	1 11	X-8	11	Date Life	1.10
1.1.2.1.1	Đ	- 60	100	- G		10	Pages 818	140
	50	10	100			21	Form SCR.	UC .
4	Ð	82	100	0		E	1000002	UK.
				-				
Read Print.								Allh
	•							
	~							
	- -							
Cours	+ 4	1000	•					
cour	ս լ	.000						

Count: Create the number counts of streams generation Apply: Apply to take effect.

3.4.2.4 Capture Criteria

Click item below to view the Capture Criteria configuration window.



The configuration is the same as selection in operation menu or toolbar as below



System shows the configuration window. Users can configure the criteria that they want to capture, from protocol or SDFR aspects

Protocol

Different protocols can be combined as unique criteria



Port A : Capture Criteria									
Protocol									
Capture all packets A									
	Network C		Protocol D						
🗖 Broadcast	Ethernet-II	SNAP	🗖 тср						
Multicast	ARP	E BPDU							
🗖 Unicast	🗖 IPv4	🗖 None IPv4	FTP						
🗖 VLAN	🗖 IPv6	🗖 IPv4 with extension header	🗖 RTP						
🗖 Q-in-Q	🗖 IPX	IPv4 checksum error	C OSPF						
CRC error	🗖 ICMP		RSVP						
🗖 Over Size	🗖 IGMP								
🗌 🗌 Under 64 bytes	MPLS								
🗖 Pause packet	Multicast MPLS								
T X-Tag E									
Packet length filte)r								
F 🗔 Filter length 🛛 equ	ual 🔽 O	*							

A: Capture all packets: All packets are captured and sent to PC by USB port. Be attention that packet loss is possible if the captured traffic is higher than traffic allowed for USB port.

B: MAC: MAC based criteria. Packets with MAC events in the list is captured and sent to PC by USB port

C: Network: Network events criteria. Packets with network events in the list is captured and sent to PC by USB port.

D: Protocol: Protocol Type criteria. Packets with protocol type in the list is captured and sent to PC by USB port.

E: X-TAG: X-TAG is an Xtramus proprietary 12 bytes embedded tag. User can capture this kind of packets from product of Xtramus

F: Packet length filter: Capture packet (frame) length in specified range of length

SDFR:

 SDFR (Self-Discover Filtering Rules) is a technique that make capture of Ethernet easy and convenient



- User-friendly interface that the value such as source IP, destination IP and other criteria for capture and filter can be input directly without calculating mask.
- SDFR value for capture or filter includes several network event (such as DA, SA, DIP...), varied length of frame (oversized, undersized) and varied of frame/packet type (CRC error, IP checksum error...).
- Value of SDFR can be a unique value or a range of values between specified values. All packets that fit the value are captured
- Multiple filter condition can be activated easily by just clicking different options
- Displays captured packet in real-time while network is still running.
- Value of SDFR and filter criteria can be changed dynamically during capture procedure.

Port A : Capture Criteria									
Protocol	SDFR								
	DA A SA VID SIP		B DA SA	Pattern C Single Single	Mode	Patterns 00-00-00-00-00-00 00-00-00-00-00-00			
	DIP SPort DPort		VID DIP	Single Single	- -				
	DA & SA DA & SA & VID		SIP	Single					
	DA & SIP DA & DIP SA & SIP		DPort SPort	Single	-	80 •			
	SA & DIP SIP & DIP SIP & SPort		-Gloss DA:	sary Dest Sour	inatio rce Ma	n MAC Address			
	SIP & DPort DIP & SPort DIP & DPort		VID: DIP:	VLAI Dest	N ID inatio	n IP Address			
	SIP & DIP & SPort	•	DPor	t: Dest	inatio	n nort			

A: SDFR items: User can tick the items that act as criteria. When user ticks one option, some other options will be gray. It means the option what user tick has covered the range of those options in gray.

B:Pattern

- DA: Destination MAC address
- SA: Source MAC address
- VID: VLAN ID that follows 802.11Q standard
- DIP: Destination IP address



- SIP: Source IP address
- DPort: Destination port of IP address
- SPort: Source port of IP address

C: Pattern Mode: Select a pattern (Single, Pair, Range) to cover the value of criteria items.

D: Patterns: The unique value or range of values specified as the capture criteria of criteria items.

For example, user wants to capture packets with VLAN ID 1 to 10.

Protocol	SDFR	
	DA SA	<u> </u>
	SIP	

Plus

VID	Papaa		< VID < 10	
ΥID	Range	<u> </u>		•

3.4.2.5 Capture Buffer

Click item below to view the Capture Buffer configuration window.



To view the contents of captured packets, user can select the captured packets from Capture Buffer window



Port A: 0	C apture (Buffer			
Save A				B ☑ Bert Er	ror Start Capture Stop Capture
	Summary	Lenth(add CRC)	DA	SA	F
	E	F	G	Н	I
∢		Item Name		00 01 02	▶ 03 04 05 06 07 08 09 0A 0B 0
CRC Error Alignment Erro 2nd CRC (DI) IP Checksum H Bert Eror IP Fragment IP Extension UDP TCP IP	or J Entor Entor	K		L	

- A: Save: Save the captured packets to file
- B: Tick this option to capture Bert Error packets
- C: Start Capture: Starts the capture process.
- D: Stop Capture: Stop the capture process

This block lists all captured packets

- E: Summary: Summary of network items
- F: Length (add CRC): Packet length that includes CRC
- G: DA: Destination MAC Address
- H: SA: Source MAC Address
- I: Frame Data: Contents of captured frame (packet).

J: Summary: List all summry items of network. When user select a packet, the summary items that fit the packet is labels as black word, otherwise, labels as gray word that it does not fit the packet. For the example below, the selected packet is **IP** packet and it does not has the other property such as CRC Error, Alignment Error.



Summary	^
CRC Error	
Alignment Error	
Dribble Error	
2nd CRC (DI) Error	
IP Checksum Error	
Bert Eror	
IP Fragment	
IP Extension	
UDP	
TCP	
IP	-

K: Item Name: Frame view of capture packets, such as Ethernet II

3.4.3 Control Panel

Click item below to view the Control Panel window.



The configuration is the same as selection in operation menu or toolbar as below



Operation menu:

Control button of this window can control packet generation and receiving, and also view the result counter



Control Panel

A 000 Save Clear				
C	Port A	Port B	Total: 2 Ports	Operation
Tx Packet	0	0	0	Port A
Tx Byte	0	0	0	Transmit 📕 📐 💷
Tx Rate	0	0	0	
Rx Packet	0	0	0	
Rx Byte	0	0	0	Port B
Rx Rate	0	0	0	
Rx GAP Large	0	0	0	Transmit 💻 📂 💷
± Collision	-	-	-	Capture 📕 📂 🗊
± Error	-	-	-	
± Packet Size Statistics	-	-	-	All Ports
± Layer2 Packet Counts	-	-	-	Transmit 📕 📂 🗊
± SDFR(Self Discover Filtering Rules)	-	-	-	Canture
Tx Pause	0	0	0	
Tx Start Time	-	-	-	
Tx End Time	-	-	-	
First Error Time	-	-	-	
Last Error Time	-	-	-	

Control buttons

- A: Save: Save current result of counters to Excel file
- B: Clear: Clear all counters to zero and it is ready for next packet generation
- C: Counter: Counters for streams generation

Counter with \pm mark is expansible. Please click the \pm mark



Operation



This option can activate Transmit or Capture of port A, port B or port A + B individually.

Button	Description
	Stop complete procedure of transmitting or capturing.
	Start to transmit or capture procedure
11	Pause transmitting or capturing procedure. System still measure the

XTRAMUS TECHNOLOGIES[®]



statistics couter, however, the counter value is static for user to watch the status when user click the III button. When user click again, the counter status resume to real status instantly. Click this button does not affect the real counters values

3.4.4 Report

Click item below to view the Report window.



3.4.4.1 VLAN Stream Counter Window

User can specify the range of VLAN ID for each port in order to view the stream counter Click item below to view the VLAN Stream Counter window.

 E	∃ <mark>Èo</mark> Report
	X-TAG Stream Counter Window

The configuration is the same as selection in operation menu as below



Operation Menu:



VLAN Stream Counter Window									
Save	000 () Clear Hide Zero	Port A VID Ra	nge 0~ 63	•	Port B VID Ra	ange 256 ~ 319			
	Port A Packet Count	Port A Byte Count		-		Port B Packet Count	Port B Byte Count		-
0	0	0	F		256	0	0	G	
1	0	0	•		257	0	0	0	
2	0	0			258	0	0		
3	0	0			259	0	0		
4	0	0			260	0	0		
5	0	0			261	0	0		
6	0	0			262	0	0		
7	0	0			263	0	0		
8	0	0			264	0	0		
9	0	0			265	0	0		
10	0	0			266	0	0		
11	0	0			267	0	0		
12	0	0			268	0	0		
13	0	0			269	0	0		
14	0	0			270	0	0		
15	0	0			271	0	0		
16	0	0			272	0	0		
17	0	0			273	0	0		
18	0	0			274	0	0		
10	0	0		•	775	0	0		•

- A: Save: Save the current counters value to Excel file
- B: Clear: Clear the current counters value to zero
- C: Hide Zero: Hide counter items that its counter value is zero
- D: Port A VID Range: Specify the range of VLAN ID of Port A

The range is based on 64 entries once a time, so the entries are 0~63, 64~127...4032~4095.

E: Port B VID Range: Specify the range of VLAN ID of Port B

The range is based on 64 entries once a time, so the entries are 0~63, 64~127...4032~4095.

- F: Packet Counts and Bytes Counts of Port A
- G: Packet Counts and Bytes Counts of Port B

3.4.4.2 X-TAG Stream Counter Windows

User can specify the range of X-TAG ID for each port in order to view the received stream counter

Click items below to view the X-TAG Stream Counter window.

XTRAMUS TECHNOLOGIES[®]



The configuration is the same as selection in operation menu as below



Operation Menu:

X-TAG Stream Counter Window								
Save	000 Clear B	(Hide) AB Zero Port AB D	A Port A	B Port B F	XID Range 0 ~ 63	▼ Port B XID Range	64 ~ 127 🔽
		I	Current Tx Rate		Packets	Bytes	Loss Packets	S/N Miss 🔺
XID 0				0	0	0	0	
XID 1				0	0	0	0	
XID 2				0	0	0	0	
XID 3				0	0	0	0	
XID 4				0	0	0	0	
XID 5				0	0	0	0	
XID 6				0	0	0	. 0	<u> </u>
•								F
Port B								
			Current Tx Rate		Packets	Bytes	Loss Packets	S/N Miss 📥
XID 64				0	0	0	0	
XID 65				0	0	0	0	
XID 66				0	0	0	0	
XID 67				0	0	0	0	
XID 68				0	0	0	0	
XID 69				0	0	0	0	
XID 70				0	0	0	. 0	•
•								▶

A: Save: Save the current counters value to Excel file.

B: Clear: Clear the current counters value to zero.

- C: Hide Zero: Hide counter items that its counter value is zero.
- D: Port AB: Lists counters value of port A and port B simultaneously.
- **E**: Port A: Lists counters value of port A only.
- **F**: Port B: Lists counters value of port B only.

G: Port A XID Range: XID (X-TAG ID) is the ID of Xtramus proprietary embedded tag in Ethernet frame. The range cover from 0~255 that is divided by 4 groups. If more then one port of this machine joins the test or more users use this device to join the test in the same network, different XID can be identify as different packet generator

H: Port B XID Range: The same function above that is applied to Port B



I: XID counter

	Current Tx Rate	Packets	Bytes	Loss Packets	S/N Miss	IPCS Error
XID 0	0	0	0	0	0	0
XID 1	0	0	0	0	0	0

Current Tx Rate: Current transmission rate (packets / sec)

Packets: Packets received

Bytes: Bytes received

Loss Packets: Packet loss found

S/N Miss: Sequence misses. X-TAG is able to detect the mis-ordered sequence.

IPCS Error: IP checksum error received

CRC Error: CRC error received

3.4.5 Function

Click item below to view the Function window.



3.4.5.1 DUT-Clock

In the sub-tree of Function



This device is equipped with high precision 1 ppm temperature-compensated oscillator that can generate precise speed network streams to DUT, or measures the speed rate of DUT's oscillator for speed control of network streams.

By using this application software, operator is able to measure oscillator's speed of DUT that is either faster or slower than standard speed in ppm scale, or use it as criteria to judge the result of test.





- **D**: Select Port: Select port that connect to DUT for test.
- F: Mode (Speed): Select network speed that user wants to test the DUT.
- H: RunTime(Sec): Configure the duration of the test.
- A: MHz: The frequency of Quartz Oscillator.
- **B**: ppm: ppm: faster (+) or slower (-) then standard speed. For example, +20 means 20ppm faster then standard speed
- C: Date: Date of this test.
- E: Max: Maximum value of MHz or ppm during the test.
- G: Min: Minimum value of MHz or ppm during the test.
- I: Current: Current detected value.
- J: Standard: Standard value for reference.
- K: MHz: MHz scale in this curve graph.
- L: Sec: Time (second) scale in this curve graph.



- M: Stop Test: Click this button to stop the test.
- N: Start Test: Click this button to start the test.
- P: Save: Save the test result.

3.5 Frame Editor

To create the pattern and contents of the streams what user want to generate, the utility has Frame Editor function to create what user want.



shows

Port A : Multi Streams Generation									
🛃 Save									
Number of Stre	earns 1	•							
Etroom #	Select	Length	Rate	X-1	ſAG	Append	Frame Data	Protocol	DA
stream #	Stream	(no CRC)	PPS 🝷	En	X-ID	CRC	Config	Туре	Mode
1	~	60	1000			•	Frame Edit	LLC	Fixed
					Fr	ame Edit			
Configure	related p	parameter	rs, then u	ser can d	click 💷''	amo Larc	⊥ to edit the d	etailed co	ontents in

frame.

3.5.1 Overview

This window shows all frame type that is configurable. User can also import user-defined file (*.pcap of Ethereal or Wireshark) for test directly.





3.5.1.1 Import

Click the A: 🖆 button and import the file from PC

C: Protocal Illustration: The figure shows the structure of packet/frame that will be generated. The figure is changeable, depending on the configuration of the packet/frame.

3.5.2 Frame View

This Frame View window shows the frame structure of the frame that user want to edit.





- A: Item Name: Network protocal type
- **B**: Value: the value in the protocal type
- C: Click ⊞ can expend the items in protocal type
- D: Contents of the edited frame/packet.

3.5.3 Data Link layer

Data Link Layer type of streams generation

\Begin{tabular}{c} & &						
Overview	, - Data Link Layer					
Frame View	 None 					
	C Ethernet II					
	O IPX					

Data Link layer: The Data Link Layer is Layer 2 of the seven-layer OSI model of computer networking. The Data Link Layer protocols respond to service requests from the Network Layer and they perform their function by issuing service requests to the Physical Layer. Several protocols options can be chosen for the test.

3.5.3.1 Ethernet II

Ethernet II: The most common Ethernet protocol currently used on LAN



Overview Ethernet II Frame View	Data Link Layer - O None © Ethernet II O IPX
Overview Ethernet II	MAC Address Destination Address: FF-FF-FF-FF-FF Source Address: 00-00-00-00-00
Frame View	Ether Type Reserved 💌

User can configure the MAC address of DUT.

Destination Address (DA): Default: FF:FF:FF:FF:FF;FF; means broadcast frame. To use

variation of DA function, this MAC address is the start MAC address

Source Address (SA): Default: 00:00:00:00:00:00, means the MAC address of this device itself. To use variation of SA function, this MAC address is the start MAC address

3.5.3.2 Variation of DA, SA and VID

The DA and SA is variable if increase or decrease selection is selected

DA, SA of Default Multi Streams generation is fixed

Port A : Multi Streams Generation								
Save								
Number of Streams 1								
Ctroom #	DA SA VID St							St
su eani #	Mode	Range	Mode	Range	Mode	Range	IFG	
1	Fixed		Fixed		Fixed		96	99

User can click the selection and change it to increase or decrease and also specify a range of variation as the example below

D	A	SA		
Mode Range		Mode	Range	
Increase	100	Decrease	150	

Assume that the DA is 00-00-21-5C-0A-22, Assume that the DA is 00-00-21-5C-0B-22

- When increase mode is selected, the last 2 hexdecimal digits will be 22, 23, 24...till the counts of the range, for example, 100.
- When decrease mode is selected, the last 2 hexdecimal digits will be 22, 21, 20...till the

I



counts of the range, for example, 150.

3.5.3.3 IPX

IPX: Internetwork Packet Exchange (IPX) is the OSI-model Network layer protocol in the IPX/SPX protocol stack. The IPX/SPX protocol stack is supported by Novell's NetWare network operating system.

🖻				
Overview Data Link Layer -				
IPX	O None			
Frame View	C Ethernet II © IPX			

This editor of IPX will added if required.

3.5.4 Tags

_

When Ethernet II of Data Link Layer is selected, extra tag options is available.

When Ethernet II is selected. Tags option is opened

–Data Link Layer
O None
Ethernet II
C IPX
Tags
 None
O VLAN
🔿 Q-in-Q
C MPLS

3.5.4.1 VLAN



	2
Overview	-Data Link Layer -
Ethernet II	O None
	Ethernet II
VLAN	O IPX
Frame View	
	l ags
	O None
	• VLAN
	O Q-in-Q
	O MPLS

A virtual LAN, commonly known as a VLAN, is a group of hosts with a common set of requirements that communicate as if they were attached to the Broadcast domain, regardless of their physical location.

The protocol most commonly used today in configuring virtual LANs is IEEE 802.1Q.

IEEE 802.1Q adds a 32-bit field between the source MAC address and the EtherType/Length fields of the original frame. The VLAN tag field has the following format:



VLAN Tag in Ethernet Frame

To configure the VLAN for streams generation, click the VLAN Tab

	VLAN Tag Parameters
Overview	User Priority CFI VID
Ethernet II	
VLAN	
Frame View	

User priority (also called COS, class of service) and VID are most common parameter for the test

3.5.4.2 Q-in-Q



	1
Overview	–Data Link Layer –
Ethernet II	O None
	Ethernet II
Q-In-Q	O IPX
Frame View	
	lags
	O None
	O VLAN
	• Q-in-Q
	C MPLS

IEEE 802.1ad (Provider Bridges) is an amendment to IEEE standard IEEE 802.1Q-1998 and it is called Q-in-Q or Stacked VLANs



To configure the Q-in-Q for streams generation, click the Q-in-Q Tab

	S-Tag
Overview	Ether Type User Priority CFI VID
Ethernet II	88:A8 0 • Reset • 0
Q-in-Q	C-Tag
Frame View	Ether Type User Priority CFI VID

3.5.4.3 MPLS





In computer networking and telecommunications, Multiprotocol Label Switching (MPLS) refers to a mechanism that directs and transfers data between Wide Area Networks (WANs) nodes with high performance, regardless of the content of the data. MPLS makes it easy to create "virtual links" between nodes on the network, regardless of the protocol of their encapsulated data.

MPLS works by prefixing packets with an MPLS header, containing one or more 'labels'. This is called a label stack. Each label stack entry contains four fields:

- > A 20-bit label value.
- A 3-bit Traffic Class field for QoS (Quality of Service) priority (experimental) and ECN (Explicit Congestion Notification).
- > A 1-bit bottom of stack flag. If this is set, it signifies that the current label is the last in the stack.
- > An 8-bit TTL (time to live) field.

This can be defined by the configuration of this utility.



	mPLS Labels	
Overview Ethernet II MPLS Frame View	MPLS Labels	MPLS Label 0 • Experiential Use 0 • Bottom of Stack 1 • Time to Live 0 •
	Append Remove	

3.5.5 Layer 3 Header

In the payload of frame, layer 3 header as the items below is configurable

Layer 3 Header				
None	C ARP			
O IPv4	O IPX			
C IPv6	O Pause			

3.5.5.1 IPv4

	2	
Overview	Data Link Layer –	Layer 3 Header
Ethernet II	C None	O None O ARP
	Ethernet II	IPv4 C IPX
IPV4	C IPX	O IPv6 O Pause

IPv4: Internet Protocol version 4 (IPv4) is the fourth revision in the development of the Internet Protocol (IP) and it is the first version of the protocol to be widely deployed.

The structure of IP header is illustrated below



bit offset	0–3	4-7	8–15	16–18	19–31	
0	Version	Header Iength	Differentiated Services	Total Length		
32	Identification			Flags	Fragment Offset	
64	Time to Live Protocol			Header Checksum		
96	Source Address					
128	Destination Address					
160	Options					
160						
or 192+	Data					

The utility has user configurable interface to match the structure of IPv4 header

Internet Protocol Address			
Destination Address	. 0 . 0 . 0		
Source Address	. 0 . 0 . 0		
(TOS Bit 0-2) Precedence	000 - Routine	Identification	0 .
(TOS Bit 3) Delay	0 - Normal 💌	Fragment	May Fragment 💌
(TOS Bit 4) Throughput	0 - Normal 💌]	Last Fragment 💌
(TOS Bit 5) Reliability	0 - Normal 💌	Fragment Offset (x8)	0
(TOS Bit 6) Cost	0 - Normal 💌	Time to Live	64 •
(TOS Bit 3) Reserved	0	Protocl B	255 - Reserved 💌

A: Differentiated Services (DS) was originally defined as the TOS (**Type of Services**) field; this field is now defined by RFC 2474 for Differentiated services (DiffServ) and by RFC 3168 for Explicit Congestion Notification (ECN), matching IPv6.

B: Most common protocols numbers are listed below and the utility has detail configuration of these protocol.

- 1: Internet Control Message Protocol (ICMP)
- 2: Internet Group Management Protocol (IGMP)
- 6: Transmission Control Protocol (TCP)
- 17: User Datagram Protocol (UDP)



IPv6: This protocol will be supported later.

3.5.5.2 ARP

	₽	
Overview	-Data Link Layer -	Layer 3 Header
Ethernet II	C None	O None 💿 ARP
	Ethernet II	O IPv4 O IPX
	C IPX	C IPv6 C Pause

ARP: Address Resolution Protocol (ARP) is the method for finding a host's link layer (hardware) address when only its Internet Layer (IP) or some other Network Layer address is known. ARP is primarily used to translate IP addresses to Ethernet MAC addresses.

The structure of ARP header is illustrated below

bit offset	0 - 7	8 - 15	16 - 31				
0	Hardware ty	rpe (HTYPE)	Protocol type (PTYPE)				
32	Hardware length (HLEN)	Protocol length (PLEN)	Operation (OPER)				
64	Sender hardware address (SHA) (first 32 bits)						
96	Sender hardware address (SHA) (last 16 bits) Sender protocol address (SPA) (first 16 bits)						
128	Sender protocol address (SPA) (last 16 bits) Target hardware address (THA) (first 16 bits						
160	Target hardware address (THA) (last 32 bits)						
192	Target protocol address (TPA)						

The utility has user configurable interface to match the structure of ARP header

Hardware Type	1 - Ethernet 💌	
Protocol Type	08:00	Sender Hardware Address 00:00:00:00:00:00
Hardware Address Length	6	Sender Protocol Address 0.0.0.0
Protocol Address Length	4	Target Hardware Address 00:00:00:00:00:00
Operation	1 - APD Request	Target Protocol Address 0 . 0 . 0 . 0
Operation		

D: IPX: Reserve function for next version



3.5.5.3 Pause

	2		
Overview	– Data Link Layer –	Layer 3 H	Header
Ethernet II	C None	O None	O ARP
	Ethernet II	O IPv4	C IPX
Pause	C IPX	C IPv6	Pause

Pause: PAUSE is a flow control mechanism on full duplex Ethernet link segments defined by IEEE 802.3x and uses MAC Control frames to carry the PAUSE commands.

	MAC Address	
Overview	A Destination Address:	01-80-C2-00-00-01
Ethernet II	Source Address:	F4-00-00-00-00-00
Pause	Pause Quanta	
Frame View	Type: 88:08	B Opcode: 00:01

A: Destination Address: 01:80:C2:00:00:01. This particular address has been reserved for use in PAUSE frames.

B: Opcode: The MAC Control opcode for PAUSE is 00:01 (0X0001 in hexadecimal)

C: A PAUSE frame includes the period of pause time being requested, in the form of two byte unsigned integer (0 through 65535). This number is the requested duration of the pause.

3.5.6 Layer 4 Header

In the payload of frame, if IPv4 is selected



Then Layer 4 header as below is configurable





3.5.6.1 TCP/IP

	2	
Overview	-Data Link Layer -	Layer 3 Header
Ethernet II	C None	O None O ARP
	Ethernet II	● IPv4 ● IPX
IPv4	O IPX	C IPv6 C Pause
TCP/IP	Tags	Layer 4 Header
Frame View	None	O None O IGMP/IP
	O VLAN	• TCP/IP
	C Q-in-Q	O UDP/IP
	O MPLS	C ICMP/IP

The Transmission Control Protocol (TCP) is one of the core protocols of the Internet Protocol Suite.

The structure of TCP segment is illustrated below. The TCP header starts after bit 160 of the IP header.

Bit offset	0–3	4-7	8–15				16–31				
0	Source port							Destination port			
32						S	equen	ce nu	mber		
64		Acknowledgment number									
96	Data offset	Reserved	CWR	ECE	URG	АСК	PSH	RST	SYN	FIN	Window Size
128		Checksum Urgent pointer							Urgent pointer		
160		Options (optional)									
160/192+		Data									

TCP Header

Flags (8 bits) (called Control bits) – contains 8 1-bit flags

- CWR (1 bit) Congestion Window Reduced (CWR) flag is set by the sending host to indicate that it received a TCP segment with the ECE flag set (added to header by <u>RFC</u> <u>3168</u>).
- ECE (ECN-Echo) (1 bit) indicate that the TCP peer is <u>ECN</u> capable during 3-way handshake (added to header by <u>RFC 3168</u>).
- URG (1 bit) indicates that the URGent pointer field is significant
- ACK (1 bit) indicates that the ACKnowledgment field is significant
- PSH (1 bit) Push function



- RST (1 bit) Reset the connection
- SYN (1 bit) Synchronize sequence numbers
- FIN (1 bit) No more data from sender

The utility has user configurable interface to match the structure of TCP segment

	TCP Paramters		
Overview	Source Port	00:00	Flags
Ethernet II	Destination Port	00:50	Urgent Pointer Valid 🗖 Reset Connection
IPv4	Sequence Number	00:00:00:00	Push Function No More Data From Sender
	Acknowledgement Number	00:00:00:00	
	Header Length (x4)	5	
Frame View	Window	08:71	
	Urgent Pointer	00:01	

3.5.6.2 UDP/IP

	2	
Overview	_Data Link Layer –	Layer 3 Header
Ethernet II	C None	C None C ARP
	Ethernet II	⊙ IPv4 O IPX
IPv4	C IPX	C IPv6 C Pause
UDP/IP	Tags	Laver 4 Header
Frame View	 None 	C None C IGMP/IP
	C VLAN	C TCP/IP
	C Q-in-Q	• UDP/IP
	O MPLS	C ICMP/IP

UDP/IP

The User Datagram Protocol (UDP) is one of the core members of the Internet Protocol Suite, the set of network protocols used for the Internet.

The structure of UDP segment is illustrated below. The UDP segment starts after bit 160 of the IP header

bits	0 - 15	16 - 31
0	Source Port	Destination Port
32	Length	Checksum
64	Da	ita



The utility has user configurable interface to match the structure of UDP segment

	UDP Paramters -	
Overview	Source Port	00:00
Ethernet II	Destination Port	00:50
IPv4	Length	8
	Checksum	00:00
ODEAL		

3.5.6.3 ICMP/IP

	7	
Overview	-Data Link Layer -	Layer 3 Header
Ethernet II	C None	C None C ARP
	Ethernet II	IPv4 C IPX
IPv4	O IPX	C IPv6 C Pause
ICMP/IP	I	J
	Tags	Layer 4 Header
Frame View	None	C None C IGMP/IP
	O VLAN	C TCP/IP
	C Q-in-Q	C UDP/IP
	O MPLS	€ ICMP/IP

ICMP/IP

The Internet Control Message Protocol (ICMP) is one of the core protocols of the Internet Protocol Suite.

The structure of ICMP segment is illustrated below

The ICMP header starts after bit 160 of the IP header

Bits	160-167	168-175	176-183	184-191
160	Туре	Code	Checksum	
192	1)	Sequence	

The utility has user configurable interface to match the structure of ICMP segment



	ICMP Paramters			
Overview	Туре [0 - Echo Replay 🛛 💌		
Ethernet II	Code [00		
IPv4	Checksum 🛛	00:00		
	ID [0		
	Sequence	0 ÷		
Ethernet II				
Frame View				

3.5.6.4 IGMP/IP

	2	
Overview	– Data Link Layer –	Layer 3 Header
Ethernet II	C None	O None O ARP
	 Ethernet II 	● IPv4 C IPX
IPv4	C IPX	C IPv6 C Pause
IGMP/IP		
	Tags	Layer 4 Header
Frame View	 None 	C None 💿 IGMP/IP
	O VLAN	C TCP/IP
	O Q-in-Q	O UDP/IP
	C MPLS	C ICMP/IP

IGMP/IP

The Internet Group Management Protocol (IGMP) is a communications protocol used to manage the membership of Internet Protocol multicast groups.

The structure of IGMP segment is illustrated below. The IGMP header starts after bit 160 of the IP header

+	Bits 0 - 7	8 - 15	16 - 23 24 -			
0	Туре	Max Resp Time	e Checksum			
32	Group Address					

The utility has user configurable interface to match the structure of IGMP segment There are three versions of IGMP



	IGMP Paramters	
Overview	Version	2
Ethernet II	Туре	Group Membership Query
IPv4	Max Response Time	8
IGMP/IP	Group Address	0.0.0.0
,		



4. Operation of NuDOG-301 with DApps-SG

To chapter tell you how to use this device to test the DUT

4.1 Control from USB Port

NuDOG-301 comes with a GUI utility software for controlling of this machine. Operator can operate this machine via USB port by Windows user interface, and also collect statistic counter and do system upgrade.

	Basic System Requirement for NuDOG-301 application software				
	Windows XP Windows Vista				
CPU	800MHz CPU	1.6 GHz, 32 bits (x86) CPU			
RAM	M 256MB RAM 1GB RAM				
HDD	20MB available space	20MB available space			
	(available space means the space for (available space means the spa				
	installation and operation) installation and operation)				

USB cable with mini-USB connector comes with the package of this machine. If operator does not have this cable, it is possible to purchase it from local electronic store. It is an industrial standard cable with standard male USB connector and standard male mini-USB connector at each side.

4.1.1 Installation of Driver

To active the USB connection, install driver for NuDOG-301 series is required The procedure below shows the installation of driver

- 1. Power On the machine
- 2. Connect USB cable to both PC and mini-USB port of NuDOG-301



3. Windows will prompt you that new USB device is found and it needs driver. Manual select the

XTRAMUS TECHNOLOGIES[®]



driver location at the folder ..**\NuDOG-301 driver** which operator gets it from Xtramus. Follow the instruction of Windows to finish the installation.

4. If driver is installed correctly, when you click icon start at right-bottom corner of Windows task bar, it shows NuDOG-301 or NuDOG-101 device



4.2 Hardware connection

To use this device, user can connect it to DUT as the illustration below



Then NuDOG-301 can generate test stream to DUT and also receive data stream from DUT for analysis

4.3 Operation of DApps-SG

2

4.3.1 Generate Test Streams to DUT

To generate the test streams, user should configure the pattern and contents of the test streams

Click SGA, System shows									
Port A : Multi Streams Generation									
Save									
Number of Streams 1									
Stroom # Select Length Rate X-TAG Append Frame Data Protocol D									
Stream (no CRC) PPS - En X-ID CRC Config Type Mode									
1	~	60	1000			~	Frame Edit	LLC	Fixed

Select the streams volume user want to generate. It can be 1~64



User can create many streams; however, only tick streams that user want to send

Stream #	Select Stream	Length
1		60
2		60

Double click value in the grid of length, then user can change the value. Select random or input the length directly.



Select the unit and input the value of the parameter that the packets will be generated.

¥	Packet per Second :	PPS
	Utilization:	%
	Line Rate:	Mbps

PPS: Packet per Second. Volume of packets that will be generated per second.

Utilization: Percentage of Wirespeed transmission

Line Rate: Mbytes per second in transmission

Tick to activate X-TAG if user needs

X-TAG	
En	
~	

Click Frame Editor to edit the pattern and contents of stream packets. Please refer to 3.5 Frame Editor about how to use frame editor

When all procedures are done, the read-only basic information at last few items if shown automatically

Protocol	Summary				
Туре	IFG	IBG	Frames		
LLC	96	96	1000		
LLC	96	96	1000		

Then input count and click Apply to take effect.	
Count 4000	



4.3.1.1 Start to generate test streams

When all configurations is done, click Control Panel on Toolbar



Save Clear				
	Port A	Port B	Total: 2 Ports	Opera
x Packet	0	0	0	Port A
x Byte	0	0	0	Transmit
x Rate	0	0	0	Continue [
tx Packet	0	0	0	
x Byte	0	0	0	Port B
x Rate	0	0	0	
x GAP Large	0	0	0	Transmit 📗
Collision	-	-	-	Capture
Error	-	-	-	
Packet Size Statistics	-	-	-	All Ports
Layer2 Packet Counts	-	-	-	Transmit
SDFR(Self Discover Filtering Rules)	-	-	-	Capture
x Pause	0	0	0	
x Start Time	-	-	-	
x End Time	-	-	-	
irst Error Time	-	-	-	
ast Error Time	-	-	-	

Click control button on operation button to control the packet generation Expend sub-item counter to see more details of counters.

4.3.2 Capture Specified Packets

To capture packets/frames of incoming streams to PC via USB port, configure capture criteria is required.

Click Cap.C A ' button on toolbar. The system shows the capture criteria settings



Port A : Capture Criteria					
Protocol	SDFR				
Capture all pack	ets				
MAC	Network		-Protocol-		
🗖 Broadcast	Ethernet-II	SNAP	🗖 ТСР		
🗖 Multicast	ARP ARP	E BPDU	🗖 UDP		
🗖 Unicast	IPv4	None IPv4	FTP		
🗆 VLAN	IPv6	IPv4 with extension header	🗖 RTP		
🗖 Q-in-Q	IPX	IPv4 checksum error	C OSPF		
CRC error	ICMP		RSVP		
🗖 Over Size	🗖 IGMP				
🗌 🗖 Under 64 bytes	MPLS				
🗖 Pause packet	Multicast MPLS				
🗆 X-Tag					
Packet length filter					
Filter length equal 🔽 🖸 🐺					

User can configure criteria of Protocol, SDFR according to section 3.4.2.4 Capture Criteria

Then Click Capture Buffer of selected port



Start capture from the Capture Buffer window



Star	t Cap	ture	Stop Capt	ure	
Port A :	Capture	Buffer			
Sere .					
101157 (137%	10				Effect Brox Stat Capture Stop Capture
1	Summary	Lanth(add CRC	DA	SA	Frame Data
1	HIT	64		03 10 00 00 10 10	\$1 60 00 18 58 00 45 00 00 14 80 00 00 08 40 FF 79 BC 00
	HIT	64	FT ST IT ST ST IT	03 00 00 00 10 00	#1 60 00 M 58 00 45 00 00 14 80 00 00 08 40 FF 75 FC 0
	HIT	64	FT IT IT IT IT IT IT	03.00 00 00 10.00	81 60 00 88 88 00 45 80 00 14 80 00 90 08 40 FF 79 8C 0
4	HIT	64		03 00 00 00 00 00	81 60 00 38 08 00 45 00 00 14 60 00 00 08 40 FF 79 FC 01
	HET	64	FT IT IT IT IT IT	03 00:00:00 00:00	\$1 50 00 31 10 00 45 00 00 14 50 00 00 05 40 FF 75 EC 0
	HIT	64	FT FT FT FF FF FF	03 88 00 08 88 50	#1 60 00 HE 05 00 45 00 00 14 80 00 00 08 40 FF 79 EC 0
1	HET	64	87 . FT . TT . FT . FT . FY	03 00 00 00 10 00	#1 60 00 HE 18 00 45 80 00 14 80 00 35 88 40 FF 75 BC 0
	HET	64	TT IT IT IT IT IT	03 00:00 00 10:00	81 60 00 38 88:00 45 80 00 14 80 00 98 88 40 57 79 EC 0
9	HET	64	FF FF FF FF FF FF	03 00 00 00 10 00	81 60 00 84 00 00 41 00 00 14 60 00 00 08 40 FF 75 8C 0
30	HET	64	FT TT TT FT FT TT	03 00:00 00 80 00	81 60 00 NI 00 00 45 00 00 14 80 00 00 08 40 FF 79 EC 0
15	HET	64	FT FT FT FT FT FT	03 00 00 00 10 00	81 60 00 31 10:00 45 00 00 14 ED 00:00 08 40 FF 75 EC 0
·		1 95			
Summer		+ ben kare	-	Value	
CRC Drop Alighment Dribble (m 2nd CRC G P Checkso field filor P Coechou field filor P Coechou field filor ficb	Enor Of XG Kinor In Direct In	B Cleared Source Trois Source	18 witten K WAN Faal Local Area Network North P T F F F F Samuel Protocol f f Samuel	International de la composition Contrata de la contrata de la composition Contrata C	A DESTRUCTOR A F AT A A 5 A 5 A 7 A 7 C 00 00 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
P		· A minimum	ALL DECKS		3 A A A A A A A A A A A A A A A A A A A

The result of captured frame is shown on Capture Buffer window.

4.3.3 View counter of captured packet and others

User can view the counters of captured packet by SDFR criteria

Click Control Panel on Toolbar



Expand SDFR sub-counter item by clicking "+" of **SDFR(Self Discover Filtering Rules)**, user the see the packet counts that is captured by SDFR criteria

User also can see conters of other events.

SDFR(Self Discover Filtering Rules)	-	-	-
- SDFR DA	3,900	1,950	5,850
- SDFR SA	0	0	0
- SDFR VID	1,950	3,900	5,850
- SDFR Q-in-Q	0	0	0
- SDFR MPLS	0	0	0
- SDFR Source IP Addr.	0	0	0
- SDFR Destination IP Addr.	0	0	0
- SDFR Destination Port	0	0	0
SDFR Source Port	0	0	0