

NETROPY[®] TRAFFIC GENERATION: TRAFFICENGINE USER'S GUIDE

Version 1.6



APPOSITE
— TECHNOLOGIES

Netropy® Traffic Generation TrafficEngine User's Guide

Revision 1.6, November 2023

Apposite® Technologies LLC

4223 Glencoe Ave, Suite B121
Marina Del Rey, CA 90292 USA
1.310.477.9955
info@apposite-tech.com
www.apposite-tech.com

Copyright ©2005-2023 Apposite Technologies LLC. All rights reserved. Apposite, Linktropy, and Netropy Network Emulators and Traffic Generators are registered trademarks of Apposite Technologies LLC. The Apposite logo and "WAN Emulation Made Easy" are trademarks of Apposite Technologies LLC. Android and the Google Play logo are trademarks of Google Inc.

Part No. DOC-UG-NNE-3c

CONTENTS

Contents.....	3
1 Overview.....	5
1.1 TrafficEngine Configuration.....	5
1.2 TrafficEngine Operation	5
2 Installation and Set-Up.....	7
2.1 Preparation.....	7
2.2 Hardware Installation	7
2.3 IP Address Configuration via the Netropy Traffic Generator GUI	7
2.4 IP Address Configuration via the Serial Console.....	8
3 Configuration.....	9
3.1 Ports	9
3.2 Hosts.....	9
3.3 Streams.....	9
4 Ports	10
4.1 Ports Overview.....	10
4.2 Port Reset.....	10
5 Test Beds	12
5.1 Test Beds Overview.....	12
5.2 Configuring Test Beds.....	12
6 Test Bed: Port Reservation	14
6.1 Port Reservation Overview.....	14
6.2 Adding Ports.....	14
6.3 Auto-Negotiated Speed.....	15
6.4 Changing Bandwidth Utilization	15
6.5 Changing Configured Line Rate.....	15
6.6 Changing Metric/Unit	16
6.7 Changing Mode.....	16
6.8 Changing Port Mapping	17
7 Test Bed: Host Configuration.....	18
7.1 Host Overview.....	18
7.2 Configuring MAC Address	18

	7.2.1	Random MAC Address	18
	7.2.2	Custom MAC Address.....	19
7.3		Configuring IP Address.....	19
	7.3.1	Random IP Address	19
	7.3.2	Custom IP Address.....	20
7.4		Configuring Gateway.....	20
7.5		Configuring Number of Hosts	21
7.6		Configuring Encapsulation Type.....	22
	7.6.1	VLAN.....	22
	7.6.2	QinQ/802.1ad.....	22
8		Test Bed: Stream Configuration	23
	8.1	Stream Overview	23
	8.2	Adding Streams.....	23
	8.2.1	Pre-Defined Streams	24
	8.3	Configuring Stream Settings	24
	8.3.1	Setting Port	25
	8.3.2	Clone Existing Streams	26
	8.3.3	Configuring Ethernet Header Options	26
	8.3.4	Configuring IP Header Options	27
	8.3.5	Configuring TCP Header Options	28
	8.3.6	Configuring State	29
	8.3.7	Configuring Traffic Rate.....	30
	8.3.8	Configuring Frames	30
	8.3.9	Burst.....	31
9		Test Bed: Traffic Configuration.....	32
	9.1	Traffic Configuration Overview	32
	9.2	Traffic Profile Configuration	32
	9.2.1	Updating Traffic Profile	33
	9.2.2	Changing Ports.....	33
	9.3	Load Profile Configuration.....	34
	9.3.1	Updating Test Duration.....	34
	9.3.2	Changing Iteration	35
10		Test Bed: Summary.....	36
	10.1	Configuration Summary.....	36
	10.2	Host Configuration.....	36

10.3	Load Profile Configuration.....	37
10.4	Start Test.....	38
11	Test Bed: Statistics.....	39
11.1	Aggregate Statistics.....	39
11.2	Statistics Per Streams.....	43
11.3	Offline Analyzer.....	44
11.4	Definitions: Aggregate Statistics.....	46
11.5	Definitions: Statistics Per Stream.....	47
12	Test Settings.....	49
12.1	Play/Pause/Stop.....	49
12.2	Clear Statistics.....	49
12.3	Start Packet Capture.....	50
13	Logs.....	51
13.1	Logs Overview.....	51
13.2	Managing Logs.....	51
13.3	Log Files.....	52
14	Administration.....	53
14.1	User Settings.....	53
14.2	Port Settings.....	54
14.3	Capture Settings.....	55
14.4	License Settings.....	55
14.5	Software Settings.....	56
14.6	Advanced Settings.....	56
14.7	Time Zone.....	57
14.8	Signature.....	57
14.9	DNS Queries File.....	58
14.10	Multisite AppStorm/AppPlayback Sync Port.....	58
14.11	Logging Frequency.....	58
15	Command Line Interface.....	60
15.1	CLI Help.....	60
15.2	CLI Top Level Commands.....	61
15.3	RADIUS Management Commands.....	62
15.4	LDAP Management Commands.....	63
16	Protocol Guide.....	64
17	Security.....	66

17.1	Users and Passwords.....	66
18	Apposite Support.....	67
18.1	Registration.....	67
18.2	Customer Support.....	67
Appendix A: Apposite End User License Agreement.....		69

1 OVERVIEW

Apposite Technologies would like to thank you for purchasing the Apposite Technologies TrafficEngine. This User's Guide is intended to describe the proper installation, configuration, and operation of this product. Please reference the *Quick Start Guide* and *Hardware Guide* for additional information. The Quick Start Guide may be used to facilitate initial configuration, and the Hardware Guide to outline the specific hardware components for each model.

1.1 TrafficEngine Configuration

The Netropy Traffic Generator must be configured through the browser-based Graphical User Interface (GUI) or using the CLI. The recommended browser is Google Chrome using HTTP or HTTPS.

1.2 TrafficEngine Operation

The configuration and use of the TrafficEngine requires the following configuration steps accessed using the system's GUI:

1. **Open the GUI**
Connect to the Netropy Traffic Generator using the default IP/Hostname assigned. Login using your user account credentials.
2. **Reserve Ports**
Reserve the specified quantity of ports you will need for your test.
3. **Create Test Bed**
Name and select TrafficEngine to configure a new test bed.
4. **Configure Ports**
Configure the Line Rate, Bandwidth Utilization, Mode, and Port Mapping for each port.
5. **Configure Hosts**
Assign Mac Addresses, IP Addresses, and hosts to the ports created in the previous step, step 4.
6. **Configure Streams**
Add streams to the test and configure stream settings.

7. **Configure the Traffic**

Configure the hosts, clients, and traffic settings.

8. **Summary**

Verify the testbed configuration.

9. **Start the Test**

Click the "Start Test" button to begin capturing data on the test bed.

10. **Evaluate results and logs**

View the graphs and statistics to analyze and evaluate the test results. Download any logs and reports.

11. **Adjust configuration**

Alter the configuration after the initial test. This can be conducted in an effort to analyze various different configurations. All previous configuration steps from 4 to 7 can be adjusted on the same test bed.

2 INSTALLATION AND SET-UP

To configure and operate the Netropy Traffic Generator TrafficEngine through its browser-based GUI, the dedicated Ethernet management port must first be configured with an appropriate IP address and subnet mask. For convenience, the MGMT interface comes pre-configured with an IP address of 10.0.0.10 and is accessible from a directly connected host on the 10.0.0.0/255.0.0.0 subnet. The IP address and subnet mask of the MGMT interface can be changed through the Netropy Traffic Generator GUI by an account with administrator privileges or by using the CLI.

2.1 Preparation

Management of the Netropy Traffic Generator device through the GUI requires a PC running an up-to-date web browser.

Initial configuration of the management interface requires:

- ▶ a PC running a supported web browser that can be configured and placed on the 10.0.0.0/255.0.0.0 network.

2.2 Hardware Installation

The Netropy Traffic Generator appliance is designed for installation in a standard 19" rack. Refer to the *Hardware Guide* for your specific model for rack-mount installation instructions.

Plug either one or two standard power cords into the Netropy Traffic Generator, depending on your model, and turn on the power. Either a U.S. standard or a U.S. Y-power cable will be supplied with each unit. The system will be available for use within 1-4 minutes.

2.3 IP Address Configuration via the Netropy Traffic Generator GUI

To configure the MGMT interface using the Netropy Traffic Generator GUI:

- 1 Configure a PC running a supported web browser with the IP address 10.0.0.2 or another address on the 10.0.0.0/255.0.0.0 subnet.
- 2 Connect an Ethernet cable between the PC and the MGMT port on the front of the Netropy

Traffic Generator.

- 3 Open the browser on the PC and enter <http://10.0.0.10> in the address bar.
- 4 Review the End User License Agreement. The Netropy Traffic Generator GUI will be displayed once the License Agreement is accepted.
- 5 Log in using the username "admin" and password "admin" to access the administrator portal.
- 6 Click on IP management in the top right corner and select change IP. Enter your network settings and select "Apply" to change these settings.
- 7 After the management interface has been configured, use the Ethernet cable to connect the MGMT port of the Netropy Traffic Generator to the management network.

2.4 IP Address Configuration via the Serial Console

- 1 Using the provided RJ45 to DB9 cable, connect the serial port of a PC running terminal emulation software to the CONSOLE port of the Netropy. Set the serial port parameters to 9600 baud, 8 bits, no parity, 1 stop bit, and disable flow control. For more details on connecting to the serial console, see the Hardware Guide for your specific model.
- 2 Press [ENTER] to display a login prompt. At the prompt, log in as "admin", password is "admin".

```
ntg login: admin
```

- 3 Use the following commands to set the IP address, netmask, and default gateway of the Netropy management interface:

```
[ntg]> mgmt set gw <default-gateway>
```

```
[ntg]> mgmt set addr <ip-address> netmask <mask>
```

IP addresses and subnet masks are entered in dotted-decimal format. For example:

```
[ntg]> mgmt set addr 192.168.1.1 netmask 255.255.255.0
```

- 4 Once the management interface has been configured, use an Ethernet cable to connect the MGMT port of the Netropy to the management network. Open a browser and enter the IP address of the MGMT interface in the address bar. The Netropy End User License Agreement will be displayed.
- 5 Review the License Agreement. The Netropy GUI will be displayed once the License Agreement is accepted.
- 6 Log in using username "admin" password "admin".

3 CONFIGURATION

To enable efficient configuration of the Netropy TrafficEngine system, it is best to develop a fundamental understanding of some basic concepts and terminology.

3.1 Ports

A port is a physical connection from one device or host to another. Ports can be configured to adjust bandwidth, line rate, mapping, and mode. These factors will alter the rates and manner through which traffic is transmitted over a link.

Refer to Section 4 and 6 for additional information on how to configure ports.

3.2 Hosts

Netropy Traffic Generator TrafficEngine uses virtual clients and servers to simulate devices on a network.

Refer to Section 7 for additional information on how to configure hosts.

3.3 Streams

Streams are blocks of data sent by an application to a port via a specific protocol.

Refer to Section 8 for additional information on how to configure streams.

4 PORTS

4.1 Ports Overview

Ports can either be set into reserve or release status. By releasing the port, you release ownership of the port, allowing it to be accessed by other users. By reserving the port, the port is retained and can be used in a new test bed.

Note: Reserving a port will not allow any other users to manage and use this same port.

These options can be enabled by clicking the switch in the Ports section of the Home page.

To configure a test bed, the necessary ports must be selected and reserved.

Ports

Ports ID	Status	MAC Address	IP Address	Reserved By	Active Feature	Test Name	Test Status	Reserve/Release
1	UP	00:10:f3:9c:af:0b	localhost					<input type="checkbox"/>
2	UP	00:10:f3:9c:af:0c	localhost					<input type="checkbox"/>
3	UP	00:10:f3:a0:49:43	localhost					<input type="checkbox"/>
4	UP	00:10:f3:a0:49:44	localhost					<input type="checkbox"/>


 Create Testbed

Figure 1: Reserve/Release Ports

4.2 Port Reset

To reset the ports, login using admin credentials and select the Ports tab.

The Ports tab displays the status of ports and allows the administrator to manually release ports as needed. This will override any port releases and reservations made by other user accounts.

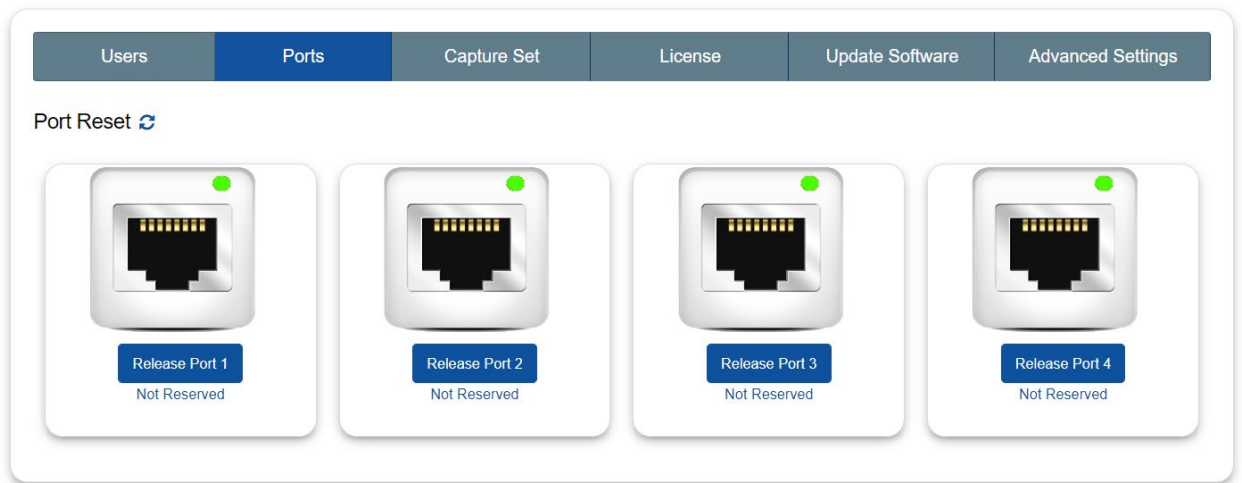


Figure 2: Port Reset

To release a port, click on the associated “Release Port X” button. As demonstrated in the figure below, this button will open a pop-up that displays the IP Address, status, speed, MAC address, and details on whether the port is reserved. By clicking “Release” the port will be released.

Refer to Section 14 for more information on Admin settings.

5 TEST BEDS

5.1 Test Beds Overview

A test bed is a platform used to configure and develop a simulated system. The test bed can be configured to emulate the specific hosts, data streams, and settings needed to accurately reflect the requirements of your system.

5.2 Configuring Test Beds

To create a test bed, select the "Create Testbed" button underneath the Port section. Select "TrafficEngine" from the menu and name the test. After naming and selecting the proper menu option, double click to add the new bed to your test environment.

The "Test Name:" field is limited to 15 characters.

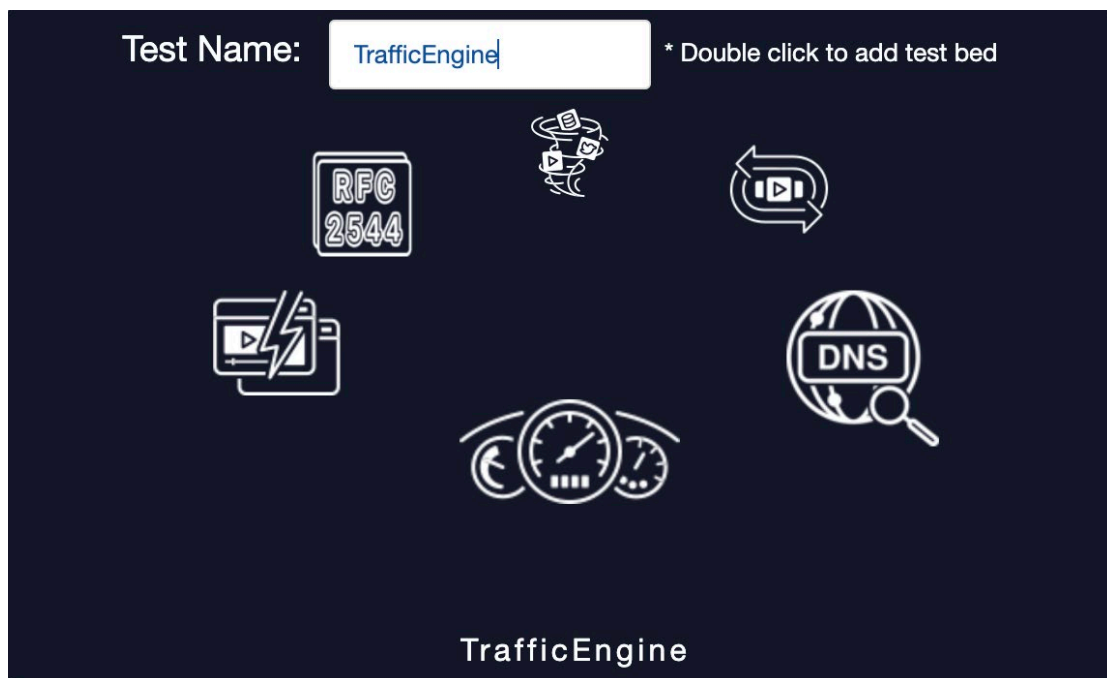


Figure 3: Naming Test Bed

After roughly 60 seconds, the new test bed should appear in the Test Bed section of the home page. Select "Configure" to begin configuring the new test. This operation will redirect you to the five-step configuration menu, starting with Drop Application Tracks.

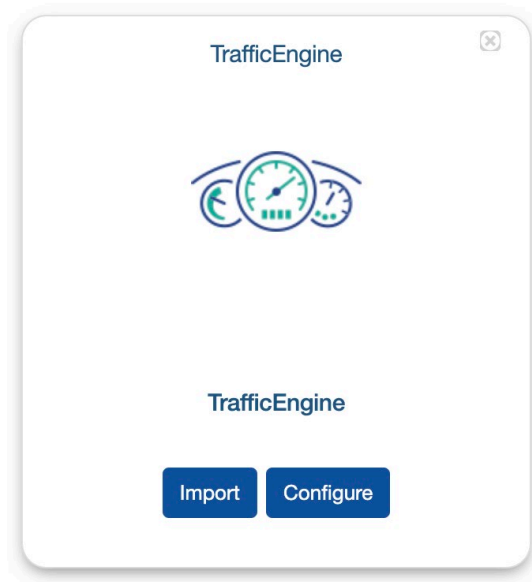
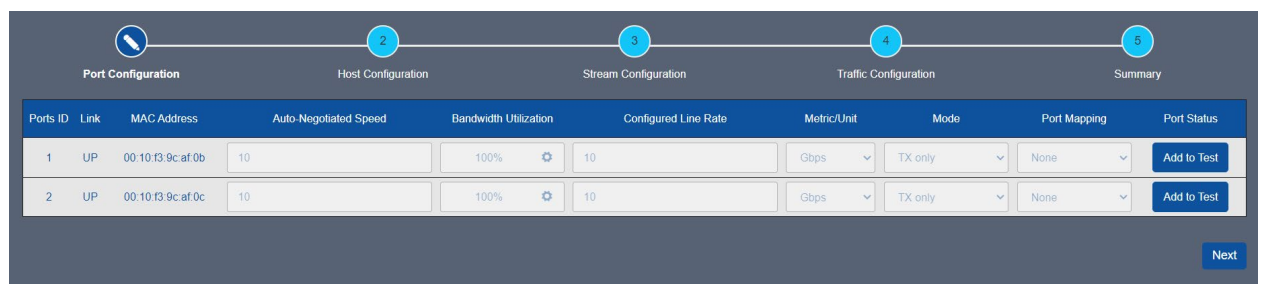


Figure 4: Configuring Test Bed

6 TEST BED: PORT RESERVATION

6.1 Port Reservation Overview

The Port Reservation menu allows you to add ports to the test bed, set up multi-site configuration, and review the current active ports, their MAC Address, Auto-Negotiated Speed, Bandwidth Utilization, Configured Line Rate, Metric/Unit Mode, Mode, Port Mapping, and Port Status.



Ports ID	Link	MAC Address	Auto-Negotiated Speed	Bandwidth Utilization	Configured Line Rate	Metric/Unit	Mode	Port Mapping	Port Status
1	UP	00:10:f3:9c:af:0b	10	100%	10	Gbps	TX only	None	<button>Add to Test</button>
2	UP	00:10:f3:9c:af:0c	10	100%	10	Gbps	TX only	None	<button>Add to Test</button>

Figure 5: Port Reservation Overview

6.2 Adding Ports

To add a Port to a test bed, select the "Add to Test" button on the right side of the Ports Configuration Tab. Selecting this button will automatically add the port to the test and be confirmed with a pop-up that the port has been added.

Add all ports that will be needed to develop your test environment.

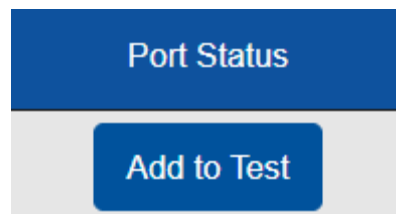


Figure 6: Add Port to Test

6.3 Auto-Negotiated Speed

By default, the Auto-Negotiated Speed is set to 10. Currently, this value cannot be altered.

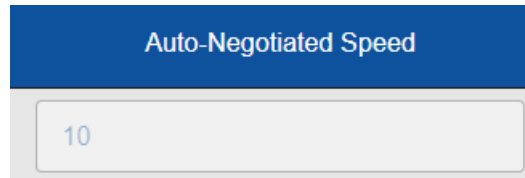
The image shows a user interface element for 'Auto-Negotiated Speed'. It consists of a dark blue header bar with the text 'Auto-Negotiated Speed' in white. Below the header is a light gray rectangular box containing the number '10' in a medium blue font.

Figure 7: Auto-Negotiated Speed

6.4 Changing Bandwidth Utilization

Bandwidth is defined as the amount of traffic that can be transmitted over the port. By default, the bandwidth utilization is set to 100%.

To adjust this number, click the gear icon underneath the Bandwidth Utilization menu. This will open a pop-up menu that allows you to enter a custom value from 0 to 100. This value will be updated automatically upon selecting the "Update" button.

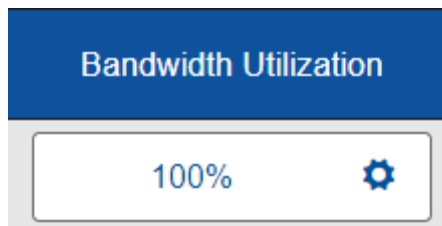
The image shows a user interface element for 'Bandwidth Utilization'. It features a dark blue header bar with the text 'Bandwidth Utilization' in white. Below the header is a light gray rectangular box. Inside this box, on the left, is the text '100%' in a medium blue font. To the right of the text is a small, dark blue gear icon.

Figure 8: Bandwidth Utilization

6.5 Changing Configured Line Rate

The Configured Line Rate is another way to configure Bandwidth Utilization by using its associated floating value. To edit this field, click on the text box and insert the value and press enter.

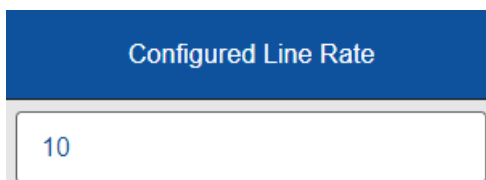
The image shows a user interface element for 'Configured Line Rate'. It has a dark blue header bar with the text 'Configured Line Rate' in white. Below the header is a light gray rectangular box containing the number '10' in a medium blue font.

Figure 9: Configured Line Rate

6.6 Changing Metric/Unit

To change the Metric/Unit select a value from the drop-down menu. The options include "Gbps", "Mbps", and "Kbps".

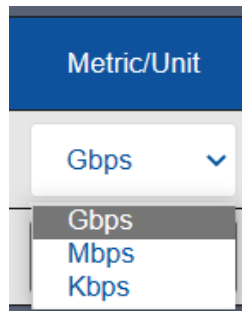


Figure 10: Metric/Unit

6.7 Changing Mode

To change the mode of the port, select an option from the Mode drop-down menu. The following mode options are available:

- ▶ TX Only:
- ▶ RX Only
- ▶ TX and RX

TX Only will only permit the port to transmit data, while RX only will permit the port to only receive data. By default, the mode will be set to TX and RX only.

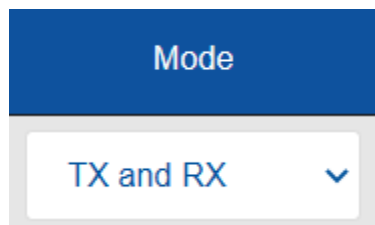


Figure 11: Mode

6.8 Changing Port Mapping

Port mapping, also known as port forwarding, is designed to redirect the data from one port to another.

To select which port to map the data to, select the designated port from the port mapping menu.

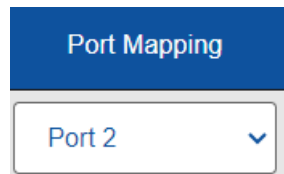


Figure 12: Port Mapping

7 TEST BED: HOST CONFIGURATION

7.1 Host Overview

The Host tab presents configuration options for all available ports.

— P1 Host Configuration

Src Mac Address: Random

Src Start Mac Address: 00:10:f3:a7:3c:40 Mac Increment Factor: 1

Encapsulation Type: None

Src IP Address: Random

Src Start IP Address: 10.0.0.2 / 27 IP Increment Factor: 1

Dest Mac Address: 80:6a:00:c4:cb:a8

Dest IP Address: 20.0.0.2

Gateway: ☐

Hosts: 32

Figure 13: P1 Host Configuration

Note: Configurations must be made for each of the associated ports selected from the prior configuration. If no changes are made, the test will be conducted using the default options.

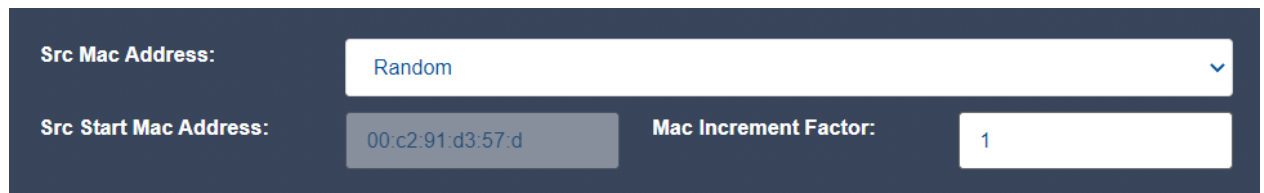
7.2 Configuring MAC Address

The Host Configuration settings allow for the configuration of either a random or custom MAC address. The processes for configuring each of these addresses are detailed in the following sections.

7.2.1 Random MAC Address

To select a random MAC address, select “Random” drop the Src Mac Address drop-down. This option will start the MAC address at the default address supplied by the system.

By default, the Mac Increment Factor will be 1. This factor is used to increment and set the MAC address values for each host. To change this value, enter in a number between 1 to 200.



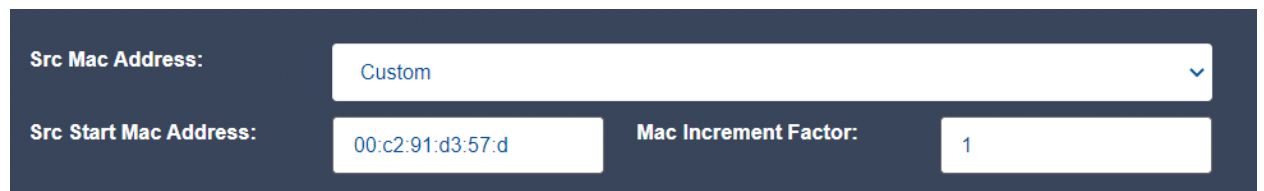
The screenshot shows a configuration panel with a dark blue background. It contains three fields: 'Src Mac Address:' with a dropdown menu set to 'Random', 'Src Start Mac Address:' with a text box containing '00:c2:91:d3:57:d', and 'Mac Increment Factor:' with a text box containing '1'.

Figure 14: Random MAC Address

7.2.2 Custom MAC Address

To enter a custom MAC address value, select "Custom" from the Src Mac Address drop-down. This will enable the MAC address field to allow a hexadecimal MAC address to be entered.

By default, the Mac Increment Factor will be 1. This factor is used to increment and set the MAC address values for each host. To change this value, enter in a number between 1 to 200.



The screenshot shows a configuration panel with a dark blue background. It contains three fields: 'Src Mac Address:' with a dropdown menu set to 'Custom', 'Src Start Mac Address:' with a text box containing '00:c2:91:d3:57:d', and 'Mac Increment Factor:' with a text box containing '1'.

Figure 15: Custom MAC Address

7.3 Configuring IP Address

The Host Configuration settings allow for the configuration of either a random or custom IP address. The processes for configuring each of these addresses are detailed in the following sections.

7.3.1 Random IP Address

To select a random IP address, select "Random" from the Src IP Address drop-down. By default, this will enable the private IP Addresses of 10.0.0.2. In addition, the default Classless Inter-Domain Routing (CIDR) address will be the value of 27, which is indicative of 32 addresses. The IP Increment factor will be a value of 1.

Src IP Address:	Random		
Src Start IP Address:	10.0.0.2	/	27
			IP Increment Factor: 1
Dest IP Address:	20.0.0.2		

Figure 16: Random IP Address

To adjust the CIDR value, simply click the drop-down and select a value between 12 and 31.

To adjust the IP increment factor, enter a custom value to the IP Increment Factor field, as shown in Figure 16.

7.3.2 Custom IP Address

To enter a custom IP address, select "Custom" from the Src IP Address drop-down and enter a new IPv4 address for the "Src Start IP Address" field. This will set the first IP address in the range which will increment based on the IP Increment Factor and subnet mask.

Src IP Address:	Custom		
Src Start IP Address:	10.0.0.2	/	27
			IP Increment Factor: 1
Dest IP Address:	20.0.0.2		

Figure 17: Custom IP Address

To adjust the CIDR value, simply click the drop-down and select a value between 12 and 31.

To adjust the IP increment factor, enter a custom value to the IP Increment Factor field, as shown in Figure 17.

7.4 Configuring Gateway

The gateway configuration is optional. By enabling the checkbox for the gateway, a new text box will appear displaying a default value.

Gateway:	<input checked="" type="checkbox"/>	GW IP Address:	20.0.0.1
-----------------	-------------------------------------	-----------------------	----------

Figure 18: Gateway Configuration

7.5 Configuring Number of Hosts

The number of hosts will adjust according to the CIDR address assigned in the IP configuration.

For example, a CIDR value of /27 will correspond to 32 hosts. On the other hand, a CIDR value of /16 will correspond to 65526 hosts.

The following figure depicts the CIDR value of 27:



Figure 19: Host Configuration (Unaltered)

To adjust the number of hosts, simply click on the outer ring of the circle to alter the number of hosts. Another option is to manually select the value in the center and enter a number. Adjusting this number will result in an allocation of fewer hosts than available on the selected subnet.



Figure 20: Host Configuration (Altered)

7.6 Configuring Encapsulation Type

By default, the Encapsulation Type value will be set to "None".

To enable an Encapsulation Type select "VLAN", "QinQ", or "802.1ad" from the drop-down menu.



A configuration form with a dark blue header. The label "Encapsulation Type:" is in white. To its right is a white text box containing the word "None" in blue, with a small blue downward arrow icon on the right side.

Figure 21: Encapsulation

7.6.1 VLAN

Once VLAN is selected, a new text box will appear labeled VLAN ID. Enter a numerical value in this field to configure VLAN.



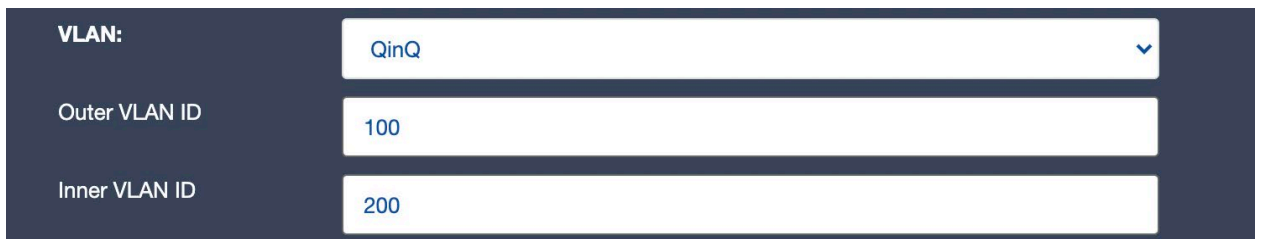
A configuration form with a dark blue header. The label "Encapsulation Type:" is in white, and the text box next to it contains "VLAN" in blue. Below this, the label "VLAN ID" is in white, and the text box next to it contains "100" in blue.

Figure 22: Enable VLAN

7.6.2 QinQ/802.1ad

If QinQ or 802.1ad is selected as the Encapsulation Type, you will be presented with additional form fields to enter "Outer VLAN ID" and "Inner VLAN ID".

Enter applicable VLAN IDs into each of these corresponding fields.



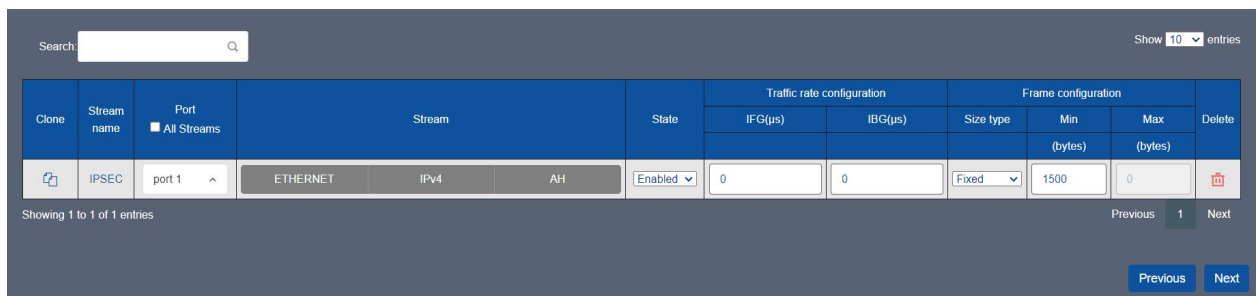
A configuration form with a dark blue header. The label "VLAN:" is in white, and the text box next to it contains "QinQ" in blue. Below this, the label "Outer VLAN ID" is in white, and the text box next to it contains "100" in blue. At the bottom, the label "Inner VLAN ID" is in white, and the text box next to it contains "200" in blue.

Figure 23: Outer and Inner VLAN ID

8 TEST BED: STREAM CONFIGURATION

8.1 Stream Overview

The Stream Configuration tab presents configuration options for all selected streams.



The screenshot shows the Stream Configuration interface. At the top, there is a search bar and a 'Show 10 entries' dropdown. Below this is a table with columns: Clone, Stream name, Port, Stream, State, Traffic rate configuration (IFG(μs), IBG(μs)), Frame configuration (Size type, Min, Max), and Delete. The table contains one entry for an IPSEC stream on port 1, configured for ETHERNET, IPv4, and AH, with a state of 'Enabled'. The traffic rate configuration shows IFG(μs) and IBG(μs) both set to 0. The frame configuration shows a fixed size type with a minimum of 1500 bytes and a maximum of 0 bytes. At the bottom, there are 'Previous' and 'Next' buttons, and a status bar indicating 'Showing 1 to 1 of 1 entries'.

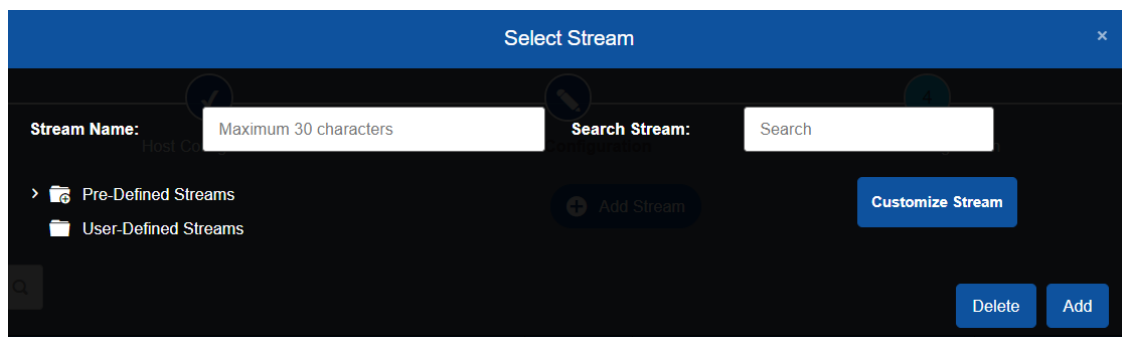
Clone	Stream name	Port	Stream	State	Traffic rate configuration		Frame configuration			Delete
					IFG(μs)	IBG(μs)	Size type	Min (bytes)	Max (bytes)	
	IPSEC	port 1	ETHERNET IPv4 AH	Enabled	0	0	Fixed	1500	0	

Figure 24: Stream Configuration

8.2 Adding Streams

To add a stream, select the "Add Stream" button in the center of the menu. Selecting this button will open a new pop-up that allows you to name and search for the specific stream you'd like to add.

Be sure to name the stream appropriately. The maximum character limit is 30.



The screenshot shows the 'Select Stream' pop-up window. It has a title bar with a close button. Inside, there are two input fields: 'Stream Name:' with a placeholder 'Maximum 30 characters' and 'Search Stream:' with a placeholder 'Search'. Below these fields, there are two expandable sections: 'Pre-Defined Streams' and 'User-Defined Streams'. In the center, there is an 'Add Stream' button. To the right, there is a 'Customize Stream' button. At the bottom right, there are 'Delete' and 'Add' buttons.

Figure 25: Add Stream

8.2.1 Pre-Defined Streams

TrafficEngine presents a set of default pre-defined Streams which can be used to simulate different types of traffic. These streams may include some of the following options:

- ▶ TCP – Transmission Control Protocol
- ▶ UDP – User Datagram Protocol
- ▶ HTTP – Hypertext Transfer Protocol – HTTP/1.1

These are only a subset of the available stream options. Select from the Pre-Defined Streams dropdown folder to view additional options.

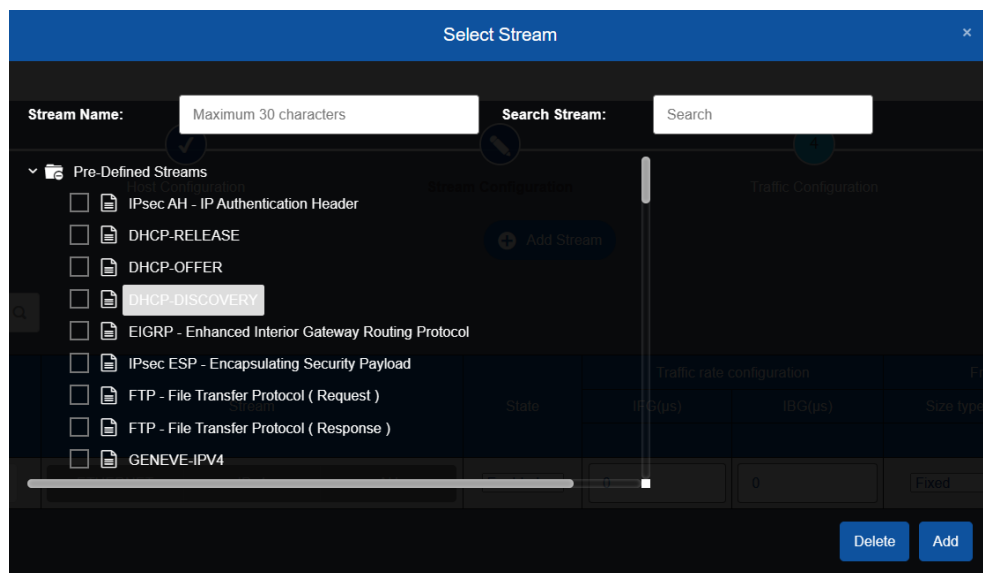


Figure 26: Pre-defined Streams

After selecting a stream, select "Add" in the lower right-hand corner of the pop-up to add this stream to the configuration.

8.3 Configuring Stream Settings

Once a stream has been added to the configuration, it will appear in the Stream Configuration Table. There are various settings that will need to be configured, including the port, stream, state, traffic rate configuration, and frame configuration.

Clone	Stream name	Port <input type="checkbox"/> All Streams	Stream			State	Traffic rate configuration		Frame configuration			Delete
							IFG(μs)	IBG(μs)	Size type	Min	Max	
										(bytes)	(bytes)	
	IPSEC	None s... ^	ETHERNET	IPv4	AH	Enabled ▾	0	0	Fixed ▾	1500	0	

Figure 27: Stream Settings

8.3.1 Setting Port

In the port options, there will be a global setting to select all ports for each of the streams. This is not enabled by default. To enable this feature, check the "All Streams" checkbox.

Port

☒ All Streams

All sele... ^

All sele... ^

Figure 28: Global Port Settings

However, if you'd like to select a very specific port, select from the drop-down under the "Port" menu in the tables. The options available will be dependent on which ports were enabled in the previous steps in Section 7.

☐ Select all

☒ port 1

☐ port 2

port 1 ^

Figure 29: Stream Configuration Ports

8.3.2 Clone Existing Streams

In the Clone section, by selecting the "Clone" icon, a copy of existing streams will be created.



Clone	Stream name
	TCP
	TCP.cp1

Figure 3028: Cloning Streams

8.3.3 Configuring Ethernet Header Options

The Ethernet button will present the SMAC Address, DMAC Address, and EtherType fields. The SMAC Address is a 48-bit value used to represent the source address, while the DMAC address is a 48-bit field used to represent the destination address. The EtherType is a 16-bit value that represents the protocol that will be encapsulated into the payload from the frame.

The SMAC and DMAC address cannot be adjusted, however, there is a drop-down to select an EtherType value. By default, the EtherType field is set to "ETHER_TYPE_IP". There are numerous available protocols to choose from, some of these options include PPPOE, IPV6, LOOPBACK, and ARP.

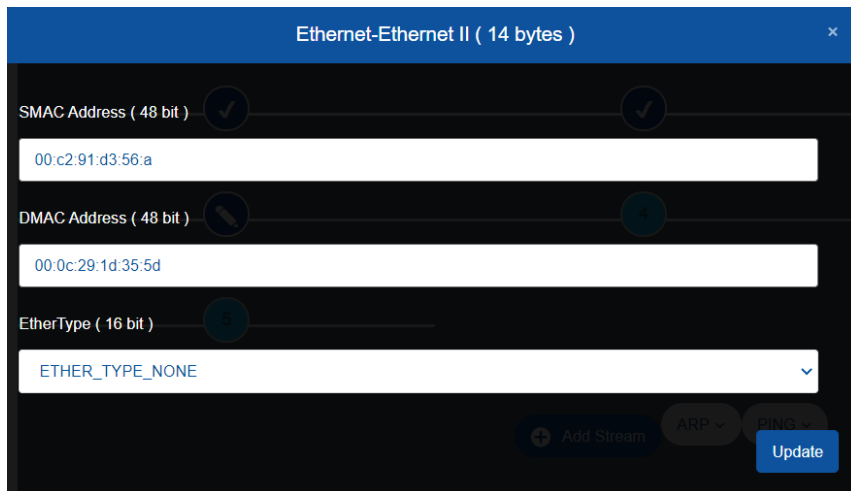


Figure 291: Ethernet Settings

8.3.4 Configuring IP Header Options

To configure the IP settings of the Stream, select IP from Stream Configuration options.

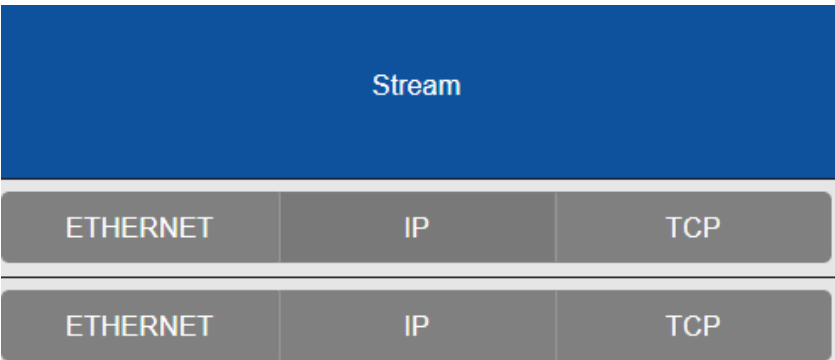


Figure 302: Stream IP Settings

Of the values presented on the pop-up menu, the TOS, Fragmentation Flags, and TTL can be adjusted.

To alter the TOS, select an option from the drop-down menu and adjust the TOS type by selecting from the check box options.

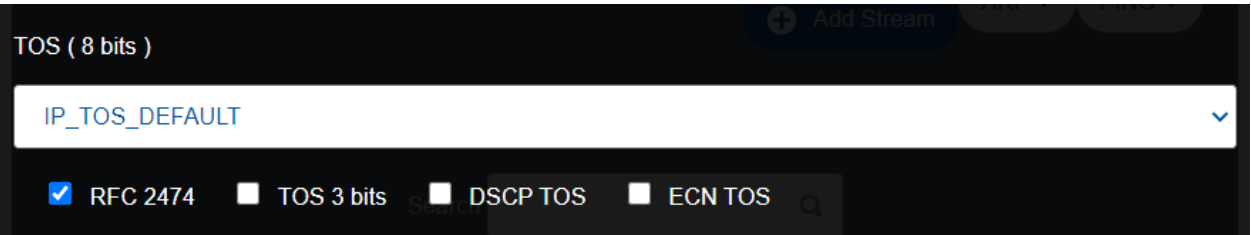


Figure 313: TOS Settings

To change the Fragmentation flags, select an option from the drop-down menu.



Figure 324: Fragmentation Flags

To alter the TTL, enter a value between 0 and 255.

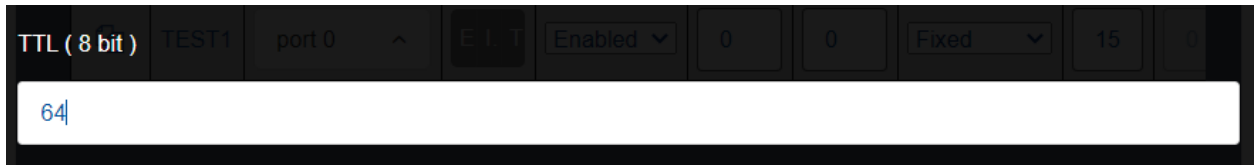


Figure 335: TTL

The following options cannot be configured and will default according to the previous settings:

- ▶ Identification
- ▶ Protocol
- ▶ Header Checksum
- ▶ Source Address
- ▶ Destination Address

To save configuration changes, select "Update".

8.3.5 Configuring TCP Header Options

To configure the IP settings of the Stream, select TCP from Stream Configuration options, as shown in Figure 21.

The only values that can be adjusted are the Flags, Urgent Pointer, Source Port, and Destination Port.

To adjust the Flags, select the required checkboxes from the menu.

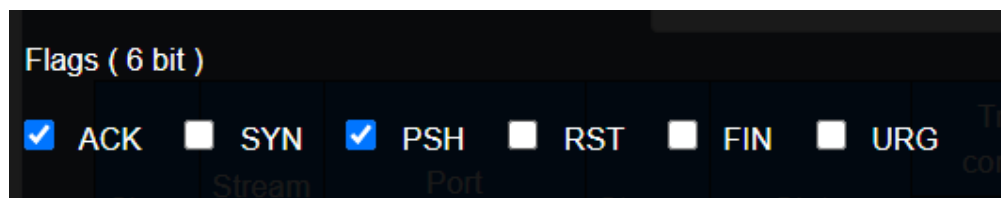


Figure 34: Stream Flags

To adjust the source and destination ports, enter the appropriate source port into the corresponding fields.

Source Port (16 bit)

2048

Destination Port (16 bit)

179

Figure 357: Stream Source and Destination Port

To adjust the Urgent Pointer, enter a 16-bit value into the corresponding field:

Urgent Pointer (16 bits)	All Streams	Stream	State	IFG(ms)	IBG(ms)	Size type	Min	Max
0								

Figure 368: Stream Urgent Pointer

The following options cannot be configured and will default according to the previous settings:

- ▶ Sequence Number
- ▶ Acknowledge Number
- ▶ Data Offset
- ▶ Reserved
- ▶ Window Size
- ▶ Checksum

To save configuration changes, select "Update".

8.3.6 Configuring State

Each stream can be enabled or disabled. An enabled state will be active when the test is running, whereas a disabled stream will not be active or impact the test results. To adjust this state, select from the drop-down menu, as shown in the figure below.

State

Enabled ▾

Figure 379: Stream State

8.3.7 Configuring Traffic Rate

The traffic configuration settings can be manually set by entering a value into either the Inter-Frame Gap (IFG) or Inter-Burst Gap (IBG) field. The most common settings range between 0 and 10ms. Values beyond 10ms will result in a drastic decrease in traffic performance and greatly impact network latency.

IFG is defined as the gap or delay between two packets when they transmit. The IBG is the gap or delay between two bursts. A burst consists of 32 packets.

The most common settings range between 0 and 10ms. Values beyond 10ms will result in drastically low traffic performance and greatly impact network latency.

Traffic rate configuration	
IFG(ms)	IBG(ms)
0	0
0	0

Figure 38: Stream Traffic Rate Configuration

8.3.8 Configuring Frames

By default, each stream's frame will be set to a fixed size with a minimum value of 1500 bytes. To alter this state, select a different size from the size type drop-down and change the minimum and maximum configuration values.

The size type options include each of the following:

- ▶ Increment
- ▶ Fixed
- ▶ Random
- ▶ Butterfly

Frame configuration		
Size type	Min	Max
	(bytes)	(bytes)
Fixed ▼	1500	0
Fixed ▼	1500	0

Figure 391: Stream Rate Configuration

8.3.9 Burst

Burst is how to send the packet. When it's set to one, it means it will send one packet at a time. Users can choose Burst size from 1 to 32. To use this feature, click on the Burst button located on the right side of the Stream configuration page. A popup window will appear with a slide bar. Drag this bar to the right to increase the number of packets. By default it set to 1.

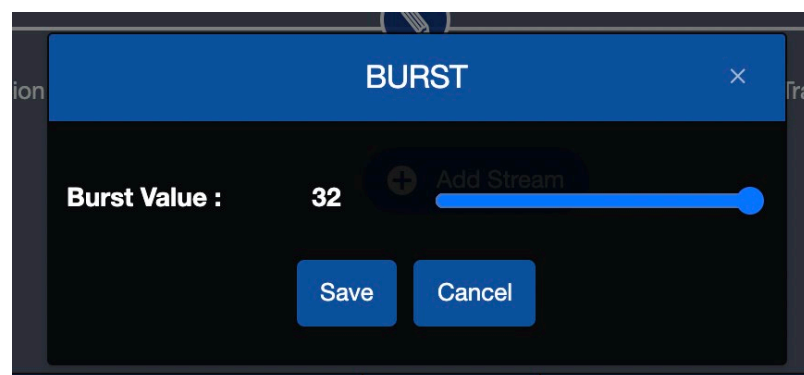


Figure 42: Burst Configuration

9 TEST BED: TRAFFIC CONFIGURATION

9.1 Traffic Configuration Overview

The Traffic Configuration tab allows for modifications to the traffic profile, time duration, and iterations for the Test Bed.

9.2 Traffic Profile Configuration

The Traffic Profile configuration allows you to make changes to the percentages of each type of traffic on each of the selected ports. Adjusting these values will impact the quantity of traffic associated with each of the previously configured streams.

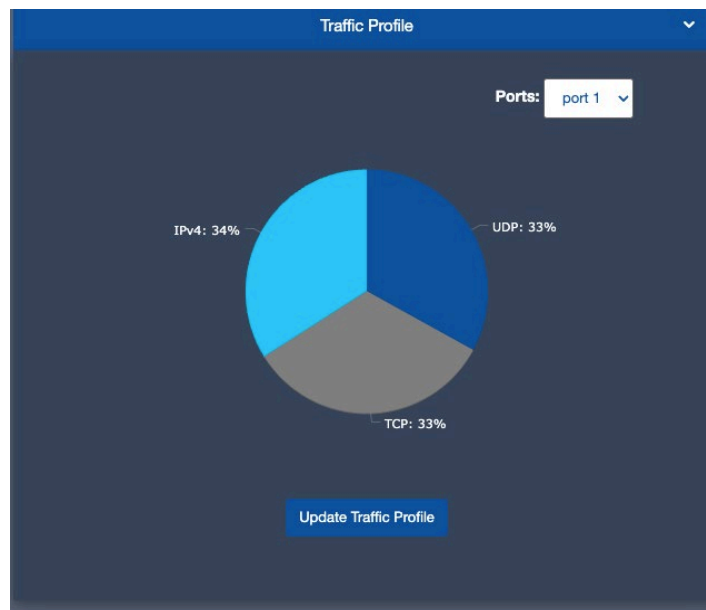


Figure 403: Traffic Profile

9.2.1 Updating Traffic Profile

To update the Traffic Profile, select the "Update Traffic Profile" button located at the bottom of the Traffic Profile graph. This will allow you to customize the amounts of traffic allocated to each designated stream.



Figure 414: Update Traffic Profile

Selecting this button will open a pop-up that displays percentages for each type of traffic. These values can be adjusted but must total to 100%. A calculation of the percentage remaining and in use will be supplied by the gray status monitors at the bottom of the screen. Select "Configure" to save the configuration changed.

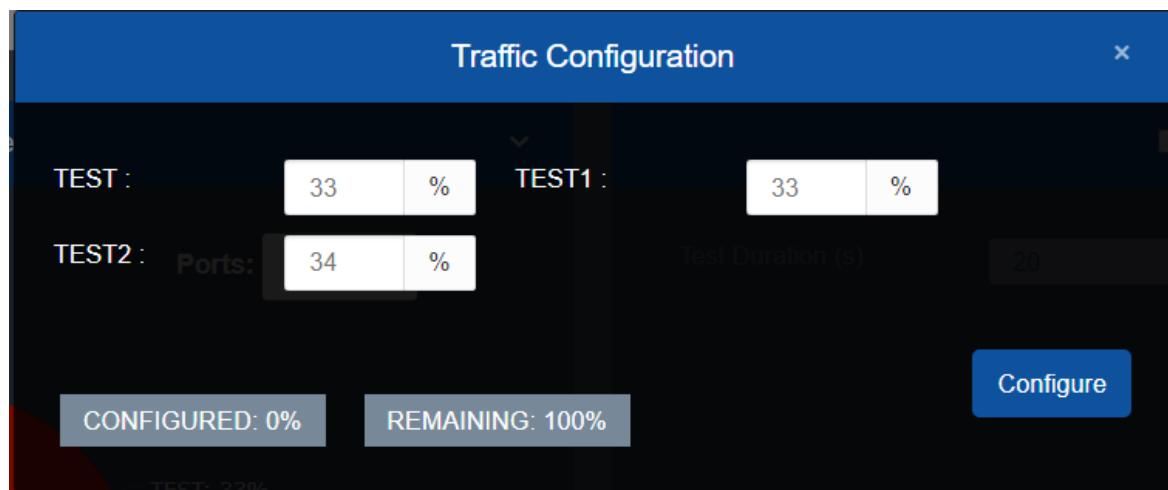


Figure 425: Traffic Configuration

9.2.2 Changing Ports

To make configurations on another port, select from the ports drop-down on the Traffic Profile graph.

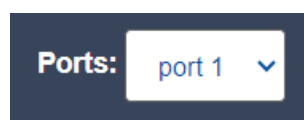


Figure 436: Changing Traffic Profile Ports

9.3 Load Profile Configuration

By default, the load profile parameters checkbox is not selected, resulting in a grayed-out menu. By selecting the checkbox, the settings become available to change. Settings include test duration and ports.



Figure 47: Load Profile Configuration

9.3.1 Updating Test Duration

To update the Test Duration settings, click the "Update Test Duration" button at the top left of the Load Profile Configuration.

The figure shows a configuration panel with a dark background. It contains two input fields: "Test Duration (s) :" with the value "20" and "Iteration :" with the value "4". Below these fields are two blue buttons: "Configure" and "Update Test Duration". The "Update Test Duration" button is positioned to the right of the "Iteration" field.

Figure 48: Test Duration Configuration

Changing the test duration impacts how long the test will run. To adjust the test duration, enter a value into the field, as shown above.


A screenshot of a configuration interface. It features a black rectangular background. On the left, the text "Test Duration (s) :" is written in a light blue font. To the right of this text is a white rectangular input field containing the number "20" in a blue font.

Figure 49: Test Duration

9.3.2 Changing Iteration

To adjust the number of times the test will run, adjust the iteration value by entering a value into the field.

A screenshot of a configuration interface. It features a black rectangular background. On the left, the text "Iteration :" is written in a light blue font. To the right of this text is a white rectangular input field containing the number "4" in a blue font.

Figure 50: Iteration

10 TEST BED: SUMMARY

10.1 Configuration Summary

The Configuration summary provides a detailed breakdown of the configuration settings selected in the previous configuration steps.

If you note any problems or discrepancies with the summary, use the "Previous button" to go back to the section that needs revisions.

10.2 Host Configuration

The Host Configuration Summary provides an overview of the configurations established for each port. The summary includes information such as the number of hosts, Start Mac address, Mac Address Type, Mac Address incrementing Factor, IP Address Type, Start IP Address, and IP Address incrementing factor.

Host Configuration		
Port 1	Number of Hosts	32
	Start Mac Address	00:10:f3:a7:3c:5f
	Mac Address Type	Random
	Mac Address incrementing Factor	1
	IP Address Type	Random
	Start IP Address	10.0.0.2
	IP Address incrementing Factor	1
	Gateway	Disabled
	Encapsulation Type	None
	Number of Hosts	32

Figure 51: Host Configuration Summary

10.3 Load Profile Configuration

The Load Profile Configuration window presents a table with the following information for each port:

- ▶ Load Profile Status
- ▶ Ramp Up(s)
- ▶ Ramp Down(s)
- ▶ Test Duration(s)
- ▶ Iteration

This information can be revised by clicking the "Previous" button at the bottom of the menu.

Load Profile Configuration		
Port	Parameters	Values
Port	Load Profile Status	Enabled
	Ramp Up(s)	4
	Ramp Down(s)	5
	Test Duration(s)	20
	Iteration	4

Figure 52: Load Profile Configuration Summary

10.4 Start Test

The test can be started by selecting the "Start Test" button at the bottom of the Summary menu. By selecting this button, the test will begin, and the webpage will reload to the statistics window.

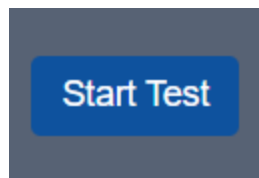


Figure 53: Start Test

11 TEST BED: STATISTICS

The Netropy Traffic Generator TrafficEngine platform provides Aggregate Statistics, Statistics Per Streams, Offline Analyzer, and Log results. All results can be viewed in the Statistics window of the GUI.

11.1 Aggregate Statistics

Aggregate Statistics provide detailed results for the test on the combined ports used in the test. This tab provides the following information:

- ▶ Statistics Table
- ▶ Port Statistics
- ▶ Packets/Second Graph
- ▶ Throughput Graph
- ▶ Latency/Jitter Graph
- ▶ % Drop Graph

The aggregate statistics table provides a tabular view of the data collected during the test.

Port	TxPkts	RxPkts	TxBits(Gbps)	RxBits(Gbps)	Latency(ms)	%Drop	TxTotalPkts	RxTotalPkts	TxTotalBits(Gb)	RxTotalBits(Gb)	AvgTxPkts	AvgRxPkts	AvgTxBits(Gb)
P1	0	0	0.0000	0.0000	0.02225	0	0	0	0.0000	0.0000	0	0	0.00
P2	0	0	0.0000	0.0000	0.02267	0	0	0	0.0000	0.0000	0	0	0.00

Figure 54: Aggregate Statistics Table

To change the metric or unit, select the proper radio button for your selection from "Gbps", "Mbps", or "Kbps".

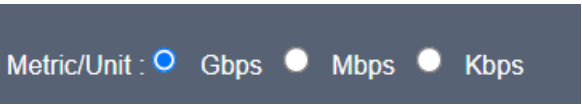


Figure 55: Aggregate Statistics Metric/Unit

To adjust the fields shown in the table, select the blue hamburger menu icon. All fields are selected by default and unchecking a field will remove it from the graph's display.

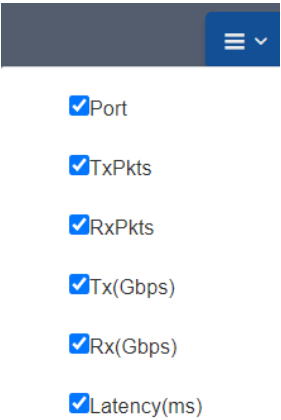


Figure 446: Statistics Filter

These statistics are further defined in Section 11.4.

The Port Statistics include, but are not limited to, Million Packet Per Second (MPPS), throughput, and latency. A sample of this output is shown in Figure 55 below.

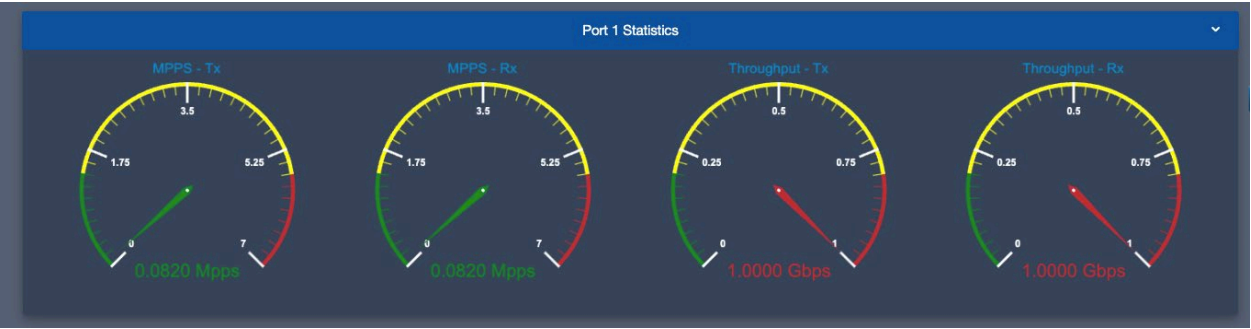


Figure 457: Port Statistics

The Packets/Second Graph provides a graphical view of the packets that travel over the network per second in each direction for both client and server.

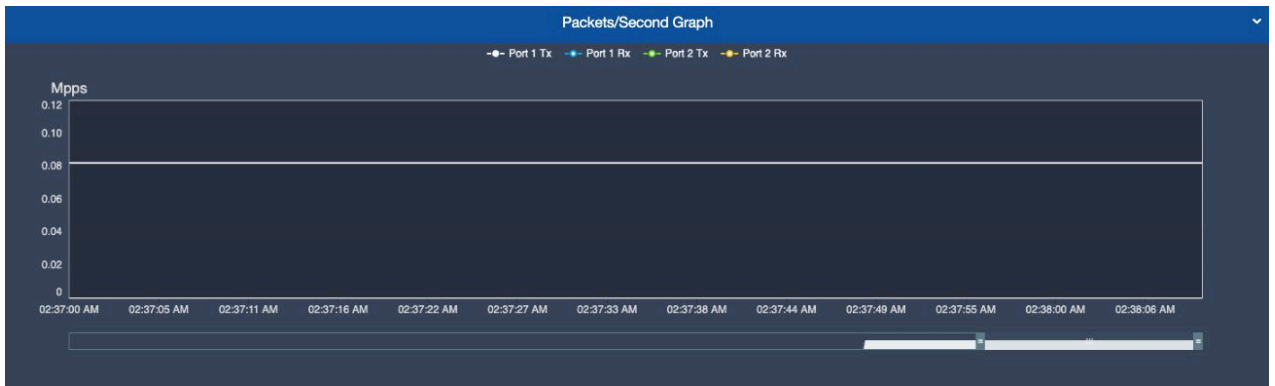


Figure 468: Packets/Second Graph

The Throughput Graph provides a graphical view of the throughput, packets sent over the network without drops, in Gbps in each direction for both client and server.

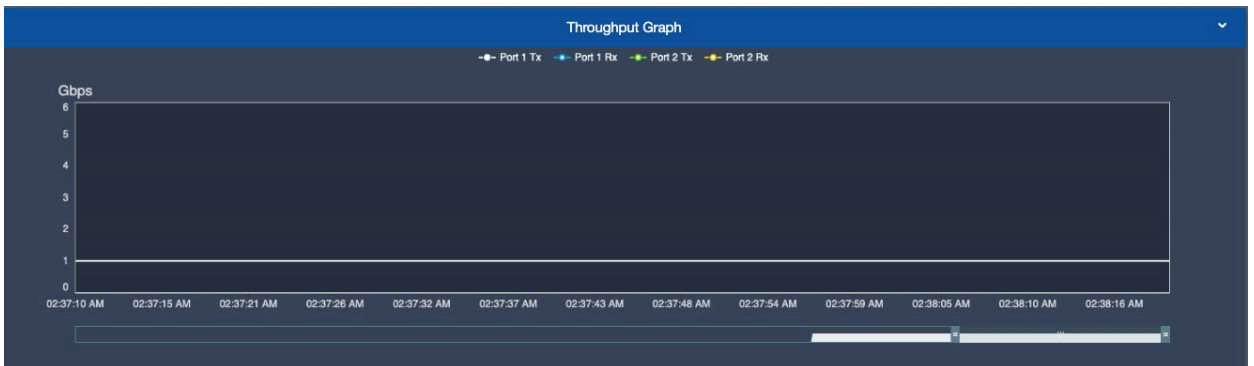


Figure 479: Throughput Graph

The Latency/Jitter Graph provides a graphical view of the throughput, packets sent over the network without drops, in Gbps in each direction for both client and server.

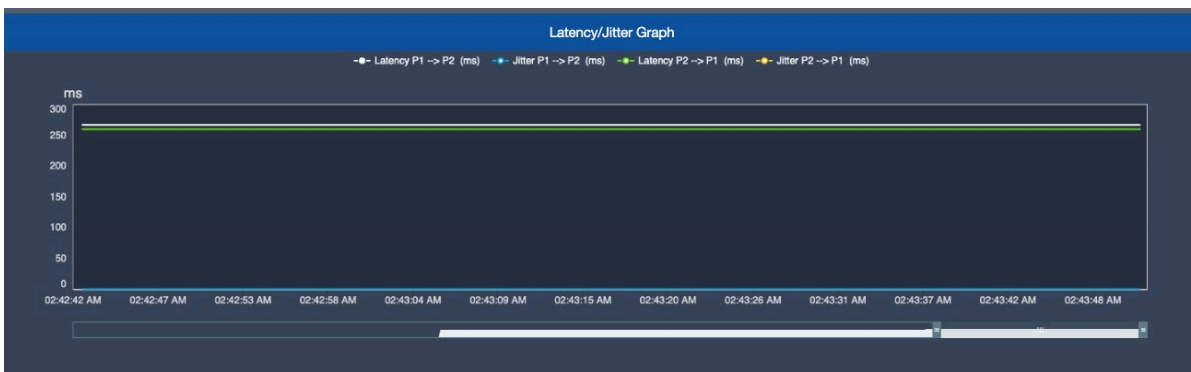


Figure 6048: Latency/Jitter Graph

The %Drop Graph provides a graphical view of the dropped packets in Gbps in each direction for both client and server.

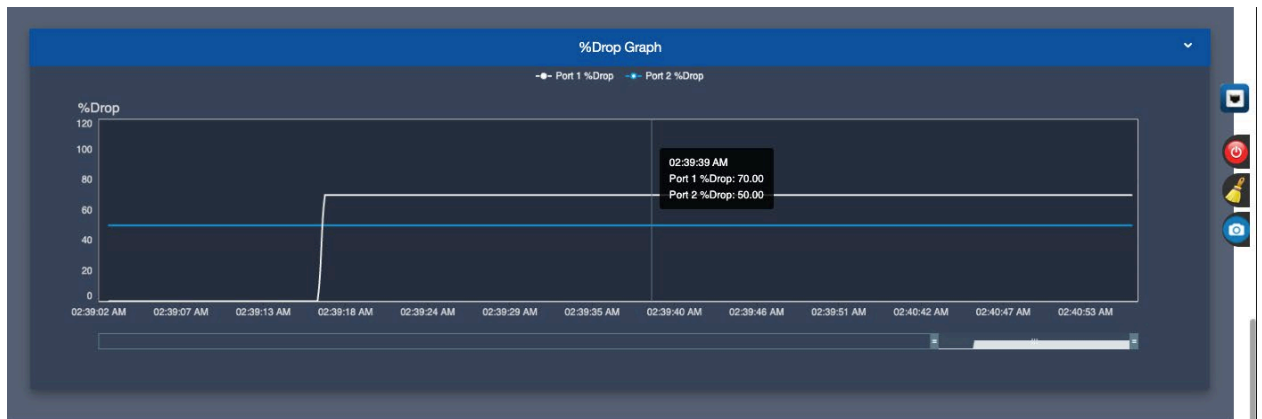


Figure 61: %Drop Graph

Each of the graphs allow you to drill-down to view a single direction for either port.

The following graph shows the Throughput for Port 2 Tx. In this view, Port 2 Tx is green and all other selections have been grayed out.

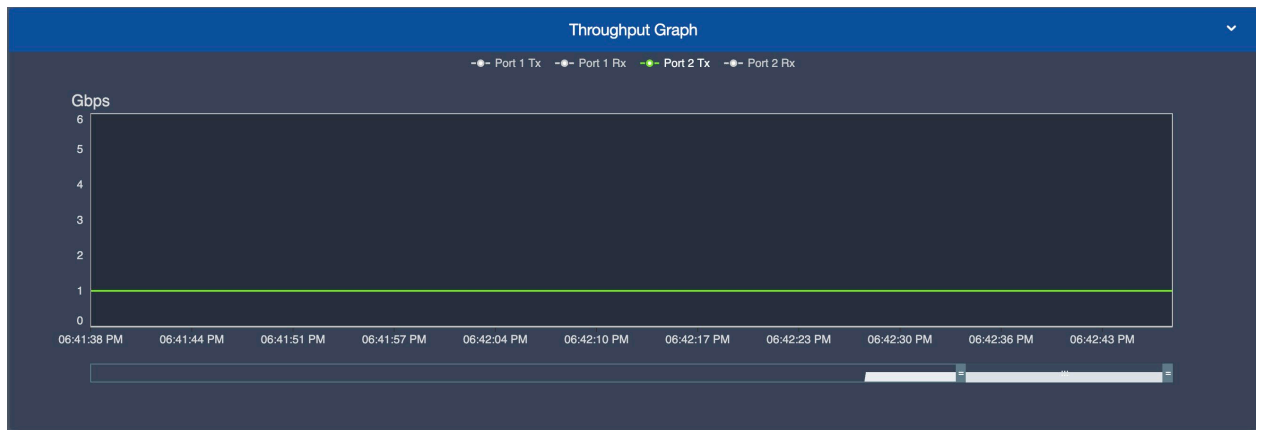


Figure 62: Throughput Graph – Port 1 Rx

This selection can be made at the top of the graph by selecting one of the conditions.

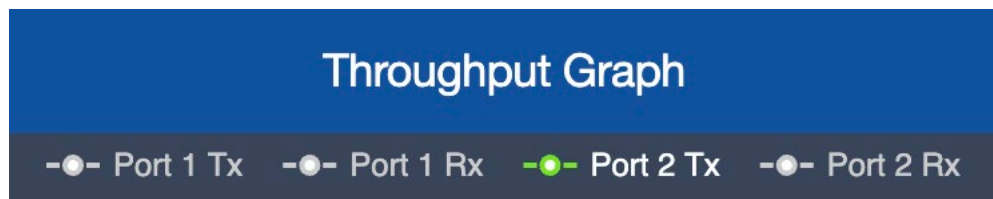


Figure 63: Graph Filters

11.2 Statistics Per Streams

The Statistics Per Stream tab provides a detailed breakdown of results for each stream on each port. These statistics are shown in a table and include information regarding the TX packets, RX packets, latency, jitter, drops, and % drops.

Stream Statistics

Search

10

Port Id	TxPkts	TxBits(Gbps)	TxTotalPkts	RxPkts	RxBits(Gbps)	RxTotalPkts	Latency(ms)					Jitter(ms)	Drops	%Drops
							Average	Minimum	Maximum	Standard Deviation (Population)	Standard Deviation (Sample)			
1	0	0.0000	0	0	0.0000	0	0	0	0	0.0000	0.0000	0	0	0

Showing 1 to 1 of 1 entries

Previous1Next

Figure 64: Statistics Per Stream Tab

These statistics are shown in a table provided and include information regarding the TX packets, RX packets, latency, drops, status, result, and direction.

To adjust the fields shown in the table, select the blue hamburger menu icon. All fields are selected by default and unchecking a field will remove it from the graph's display.

10

Figure 495: Statistics Per Stream Filter

Section: Test Bed:
Statistics

43

These statistics are further defined in Section 11.4.

To search for specific keywords from the dataset, enter data into the search field. This will filter the packets for the specified data.



Figure 506: Search

11.3 Offline Analyzer

The Offline Analyzer tab provides the following graphs:

- ▶ Packets/Second
- ▶ Throughput
- ▶ Latency/Jitter
- ▶ % Drop Graph

To download, select the download icon on the right of the graph and hover over "Download as..." to present the available download options.

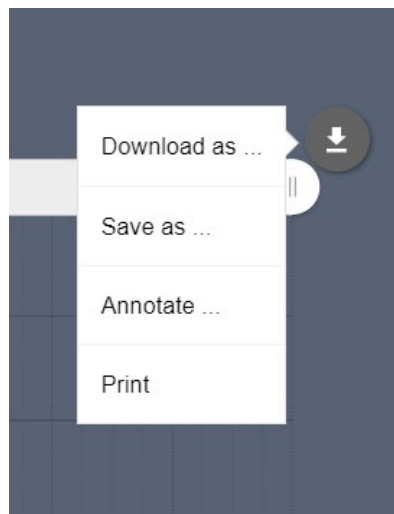


Figure 517: Downloading Graphs

Each of these graphs can be downloaded individually in either PDF, JPG, SVG, or PNG format. To select a file format, click your desired format from the menu. The selected file will be downloaded directly to your computer's default file location for downloads.

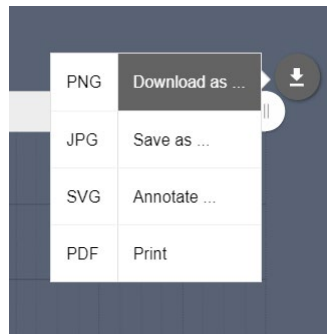


Figure 68: Download File Options

In addition, each graph can be saved as a CSV, JSON, or XSLX file. To select one of these options, hover over the "Save as..." option and select the desired file format.



Figure 69: Save As File Options

To print the graph, select the "Print" option from the menu shown in the figure above. This will open your browser's printing menu and allow you to select your default printer and settings.

These graphs also may be annotated using the built-in illustration feature. These annotated graphs can also be downloaded in the same formats. To annotate a graph, select the "Annotate..." option from the menu.

Selecting this menu option will turn the graph white and allow you to annotate the graph. Users can add shapes and text directly to the graph. In addition, users are allowed to change the color and mode of the marker and text.

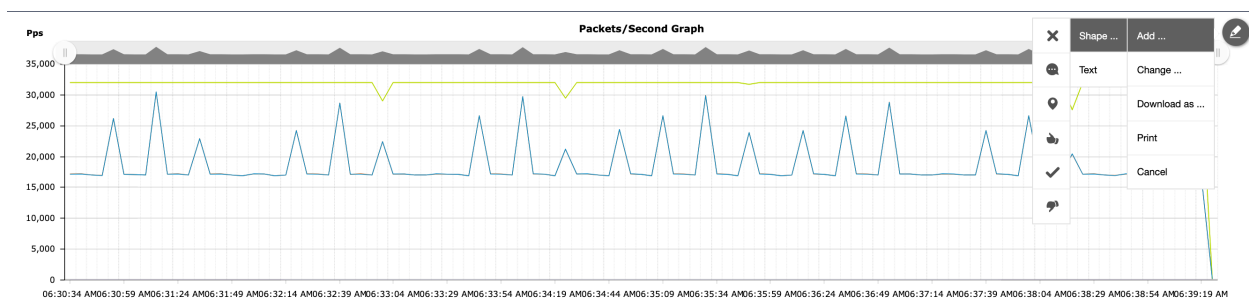


Figure 70: Annotate Graph

To change the annotated graph, hover on the edit pen on the top right corner of the graph and select "Change".

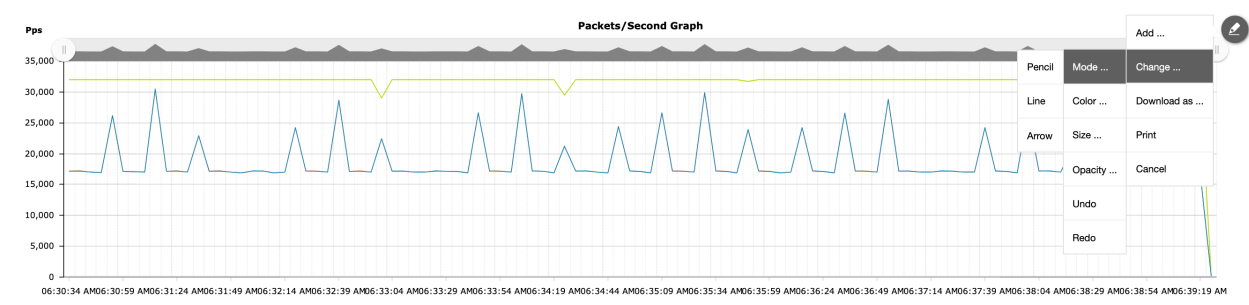


Figure 71: Change Graph

The annotated graph can be printed or downloaded in either PNG, JPG, SVG, or PDF format.

11.4 Definitions: Aggregate Statistics

The following table includes the definition of various statistics displayed in the graphs and tables provided by TrafficEngine:

Segment	Statistic	Description
	Port	The Port Number for which statistics are shown.
	Drop	The total number of packets dropped on the Port from the time test was started. The drop counter gets updated only when the test stops.
	TXPkts	The number of packets transmitted on the port in the last 1 second interval.

	RxPkts	The number of packets received on the port in the last 1 second interval.
	TXBits((Gbps)	The rate of packets transmitted (in Gigabits per second) on the port in the last 1 second interval.
	RXBits (Gbps)	The rate of packets received (in Gigabits per second) on the port in the last 1 second interval.
	Latency(ms)	The time (in milliseconds) taken by the packet to be received on the Destination port from the time it was transmitted on the Source port. This is calculated as an average for all the packets received in the last 1 sec interval.
	TxTotalPkts	The total number of packets transmitted on the port from the time test was started.
	RxTotalPkts	The total number of packets received on the port from the time test was started.
	AvgTxPkts	The average number of packets transmitted on the port per second from the time test was started.
	AvgRxPkts	The average number of packets received on the port per second from the time test was started.
	AvgTxBits(Gb)	The average rate of packets transmitted (in Gigabits per second) on the port per second from the time test was started.
	AvgRxBits(Gb)	The average rate of packets received (in Gigabits per second) on the port per second from the time test was started.

11.5 Definitions: Statistics Per Stream

The following table includes the definition of various statistics displayed in the graphs and tables provided by TrafficEngine:

Segment	Statistic	Description
	Stream Name	The user defined name for the stream.
	Port Id	The Port Number for which statistics are shown for a specific stream.

	Drop	The total number of packets dropped on the Port from the time test was started. The drop counter gets updated only when the test stops.
	TXPkts	The number of packets transmitted on the port in the last 1 second interval.
	RxPkts	The number of packets received on the port in the last 1 second interval.
	TXBits((Gbps)	The rate of packets transmitted (in Gigabits per second) on the port in the last 1 second interval.
	RXBits (Gbps)	The rate of packets received (in Gigabits per second) on the port in the last 1 second interval.
	TxTotalPkts	The total number of packets transmitted on the port from the time test was started.
	RxTotalPkts	The total number of packets received on the port from the time test was started.
	Latency Average	- The average time (in milliseconds) taken by the packets for a specific stream to be received on the Destination port from the time it was transmitted on the Source port. The average is computed over all packets that have been received till that time.
	Latency Minimum	- The minimum time (in milliseconds) taken by a packet for a specific stream to be received on the Destination port from the time it was transmitted on the Source port. The minimum time is computed over all packets that have been received till that time.
	Latency Maximum	- The maximum time (in milliseconds) taken by a packet for a specific stream to be received on the Destination port from the time it was transmitted on the Source port. The maximum time is computed over all packets that have been received till that time.
	Latency Standard Deviation (Population)	The time deviation (in milliseconds) from the Average latency computed over all the packets for a stream received till that time.
	Latency Standard Deviation (Sample)	The time deviation (in milliseconds) from the Average latency computed over all the packets for a stream received in the last 1 second interval.

12 TEST SETTINGS

The test provides options to capture PCAPs, pause, play or stop the test, and clear statistics. The following sections will provide additional details on these configurations.

12.1 Play/Pause/Stop

To adjust the play, pause, and stop settings for a test, select the power button on the right side of the screen.



Figure 522: Play/Pause/Stop Settings

Selecting this button will present a menu to select the pause, play, and stop buttons. When the test is stopped, the test bed will initiate the generation of a report. This report will be available within the Logs tab. If a test is paused, the user will be notified and provided the option to replay in the same menu.

If a test is played, the user will be provided the option to either pause or stop the test.

12.2 Clear Statistics

To clear the current statistics, hover over the broom icon on the left side of the screen and select "Clear Statistics". This action will clear all statistics shown in the available graphs but will not alter the contents of the Log files.



Figure 533: Clear Statistics

12.3 Start Packet Capture

To start a network packet capture of the traffic that occurs during your test, hover over the camera icon on the left side of the screen to present a green button labeled "Start Capture". Click this button to begin a network packet capture.



Figure 74: Network Capture

13 LOGS

13.1 Logs Overview

Logs may be collected from tests to use for analysis and review by users. The system will collect and maintain these logs for future use. These files can be found within the Logs tab of the Statistics menu.

The size of these log files will vary based on the amount of data collected and the number of packets selected within the capture. All capture files will be provided in .pcap form to ensure they are compatible with Wireshark and similar software programs.

13.2 Managing Logs

The Logs tab of the Statistics window presents a list of available reports. These reports can be downloaded or deleted.

To download a report, select the download icon on the specified file. This will download a zip folder to the default download location on your device. To delete a file from the logs, select the trash can icon on the specified file.

To delete all logs, select the "Delete All" button in the top right corner.

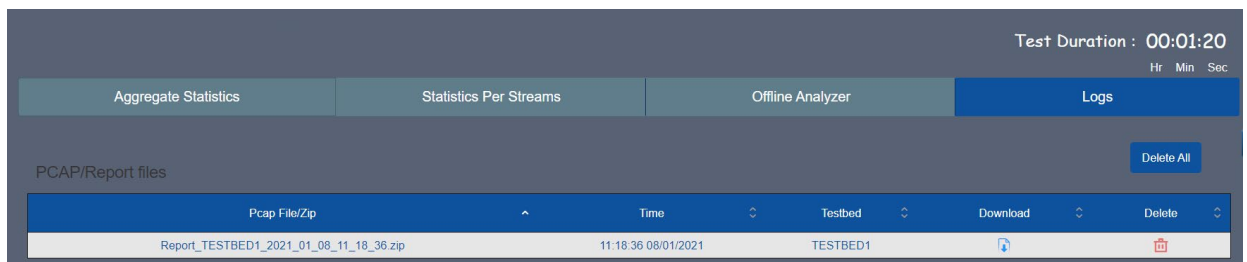


Figure 545: Logs Tab



If you select delete on a report, you will not be presented with a confirmation window. Unless previously downloaded, you cannot retrieve deleted reports.

13.3 Log Files

After a report has been downloaded, right-click the zip folder and select "Extract All" to extract these files to your selected folder and/or location. The extracted folder may include some of the following files:

- ▶ Offline Analyzer Latency (CSV)

This file includes latency data collected from the test.

- ▶ Offline Analyzer PPS (CSV)

This file includes packets per second data collected from the test.

- ▶ Offline Analyzer Throughput (CSV)

This file includes throughput data collected from the test.

- ▶ Configuration (XML)

This file includes the test bed configuration, which can be imported into the test later.

- ▶ PDF Test Report

This file includes a PDF Summary of the Test Scenario and corresponding graphs.

- ▶ % Drop Graph (JPG)

This image includes a snapshot of the percentage of dropped packets during the test.

14 ADMINISTRATION

The Netropy Traffic Generator TrafficEngine can be administered through the Administration portal accessible via browser. The administrator must log in using their administrative credentials.

14.1 User Settings

The User tab presents options to add, edit, and delete users. By default, there will only be a single user account, the administrator. To create additional accounts to manage and configure test beds, the administrator must add new users.

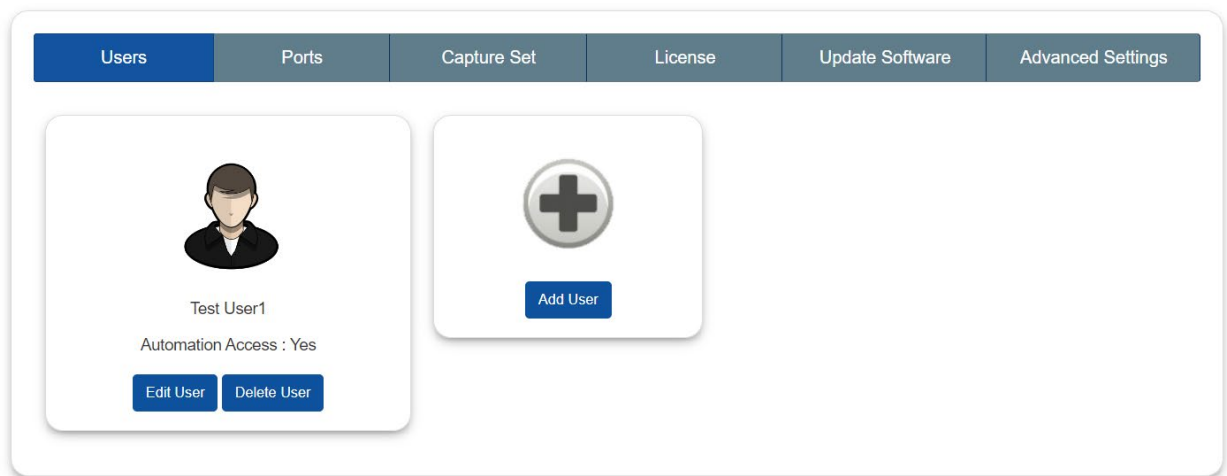


Figure 556: User Tab

When adding a new user, the following information is required:

- ▶ First Name
- ▶ Last Name
- ▶ User Name
- ▶ Email

- Password
- Automation access

The account will be created once the “Create User” button is selected. This user will then be able to access the configuration portal using their new credentials. Only the administrator will have access to these permissions. Other users will be able to make configuration changes but will not have privileges to access and manage other accounts.

14.2 Port Settings

The Ports tab displays the status of ports and allows the administrator to manually release ports as needed. This will override any port releases and reservations made by other user accounts.

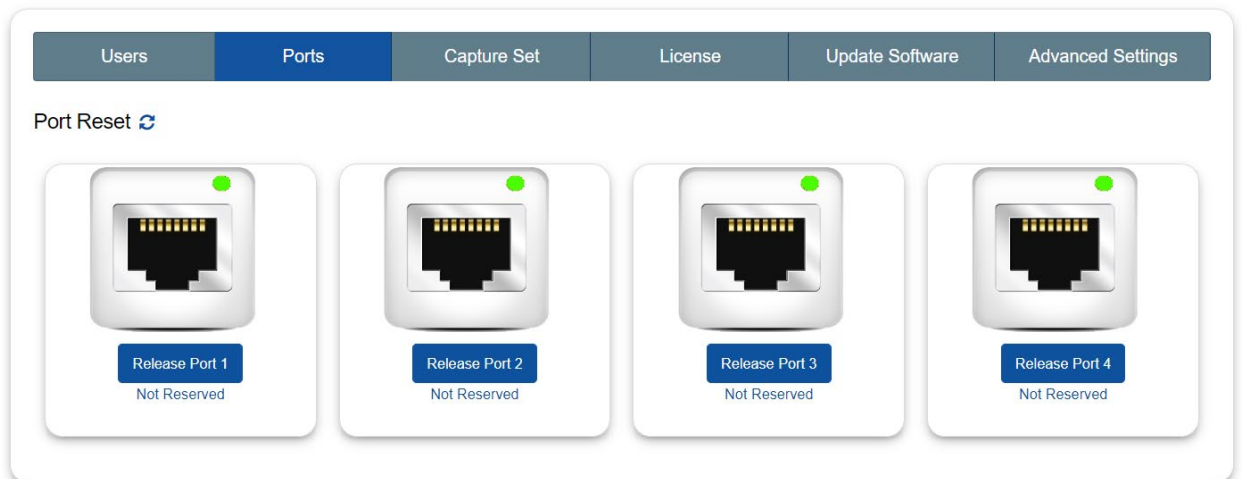


Figure 77: Port Tab

To release a port, click on the associated “Release Port X” button. As demonstrated in the figure below, this button will open a pop-up that displays the IP Address, status, speed, MAC address, and details on whether the port is reserved. By clicking “Release” the port will be released.

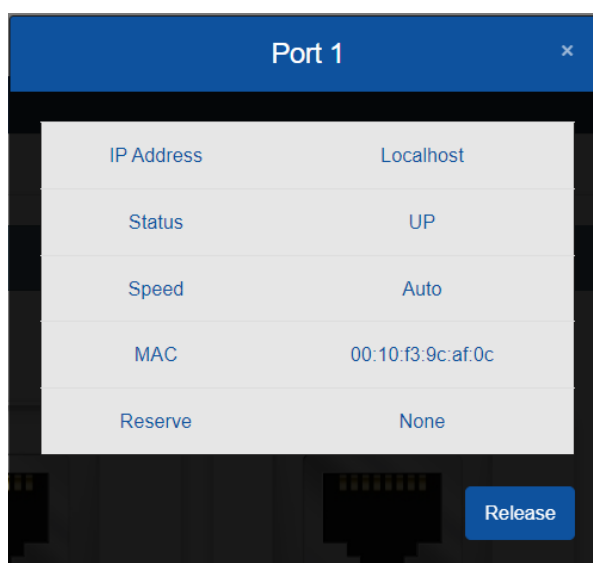


Figure 568: Release Port Settings

14.3 Capture Settings

The TrafficEngine can be configured to capture a specific number of packets during a session. By default, the number of packets to capture will be set to 100 packets. This setting can easily be altered by clicking the drop-down menu, as shown in the figure below. Options in this menu will range from 100 packets to 1,000,000 packets.

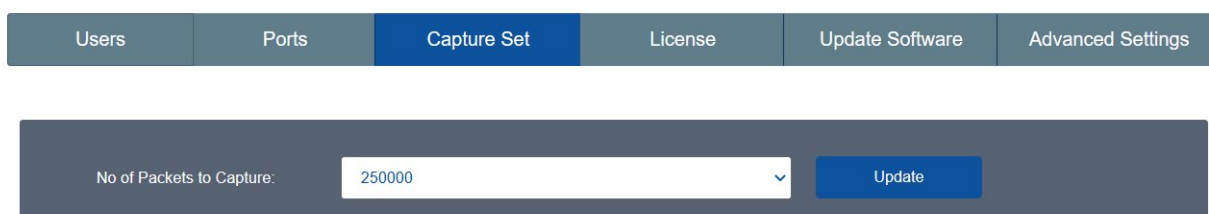


Figure 579: Capture Settings

Click "Update" to initiate these changes and ensure all future packet sessions will capture the specified number of packets.

14.4 License Settings

The License tab will display the license, license type, license validity, and the number of licensed ports. To obtain additional information on how to renew a license, visit <https://www.apposite-tech.com/renewals/> to submit a renewal request form.

To add a license key, click the "Browse" button to search for files on your device. After selecting the

applicable file, click "Open" in file explorer. Then, proceed by selecting "Upload" to upload the license key file into the system.

Users	Ports	Capture Set	License	Update Software	Advanced Settings
-------	-------	-------------	---------	-----------------	-------------------

License	Valid
License Type	TrafficEngine, AppStorm, AppPlayback, RFC-2544, SessionStrike, DNS Storm
License Validity	6 Aug, 2121
Number of Licensed Ports	2

License File

Figure 8058: License Tab

14.5 Software Settings

The Update Settings tab allows the selection of a BIN file to update the system software. To update the BIN file, select the plus button icon, and select the appropriate file on your PC. After selecting the file, the system will request a system reboot. Select "Yes" to allow the system to apply all necessary patches and updates.

Users	Ports	Capture Set	License	Update Software	Advanced Settings
-------	-------	-------------	---------	-----------------	-------------------

Upload Bin file

Figure 81: Update Software Tab

14.6 Advanced Settings

The Advanced Settings tab allows management of time zone, signature, binary search, DNS Queries File, Authentication, NAS IP, and Secret Key.

Figure 592: Advanced Settings

14.7 Time Zone

Users can select the time zone of their location. To select the time zone, click the down arrow next to the default time by the “Select Timezone” value.

Figure 83: Time Zone

14.8 Signature

The selection determines where the control information used by NTG gets stored in the packets

being transmitted.

1. **IP Options:** In this case, the control information is stored in the IP options field in the IP header.
2. **Payload:** In this case, the control information is stored in the IP Payload.

To select one of the two options, select the applicable radio button. Then, click "Update" to complete the change.



Figure 84: Signature

14.9 DNS Queries File

This is the file which consists of the lists of domain names which are used by the DNS Storm feature when sending DNS queries. DNS Storm feature cycles through this list of domain names.

Select "Browse" to choose the appropriate DNS Queries File. Then, click "Update" to complete the change after the file has been selected.



Figure 85: DNS Queries File

14.10 Multisite AppStorm/AppPlayback Sync Port

By default, the Multisite AppStorm/AppPlayback Sync Port value is set to 10000.

To update this field, please enter a new value and select "Update".



Figure 86: Sync Port

14.11 Logging Frequency

Users can select a logging frequency between 1 second and 5 seconds from the drop the dropdown and select "Update" to ensure the system changes this frequency.

For a shorter testing window, you may want to have a smaller logging frequency. Whereas, for a longer testing window, you may want to have a larger logging frequency.

A horizontal configuration bar with a dark blue background. On the left, the text "Logging Frequency :" is displayed in white. To its right is a white dropdown menu containing the text "5 sec" and a small blue downward arrow. Further to the right is a blue button with the white text "Update".

Logging Frequency : 5 sec Update

Figure 87: Logging Frequency

15 COMMAND LINE INTERFACE

The Netropy command line interface (CLI) can be accessed via the CONSOLE interface or through a Telnet or SSH connection.

The following are the only features available through the CLI:

- ▶ ARP and PING commands
- ▶ Reinitialize the unit to factory settings
- ▶ Management functions

To access the CLI, log into the device at the prompt as "**admin**" or other configured username.

15.1 CLI Help

The CLI includes several levels of help. The "**help**" command by itself displays a list of commands. "**help**" with a command name displays the syntax and options for the command.

When entering commands, the <Tab> key can be used to complete a partially entered command name. If there are multiple possible completions, pressing the <Tab> key again will display a list of options.

15.2 CLI Top Level Commands

Command	Syntax and Description
arp	arp show Displays a table of IP addresses and associated MAC addresses for the MGMT interface.
clock	clock show Displays the current system time and date.
help	{help ?} [<command>] Displays a list of available commands or syntax of a specified command. A question mark after any command also displays the syntax for that command.
init	init config Returns the configuration to factory default settings. Takes effect upon reboot unless the configuration is saved prior to reboot.
logout	logout Logout from the command line interface.
mgmt	mgmt show Displays the IP address and other management information. mgmt show ntp associations Displays the synchronization state with the configured NTP servers. mgmt set addr {dhcp addr <addr> netmask <mask>} Sets the IPv4 address and netmask of the MGMT interface either manually or using DHCP. If DHCP is enabled, DHCP sets the default gateway. mgmt set domain <domain> Sets the network domain name of the device. mgmt set gw <addr> Sets a default gateway for the MGMT interface. mgmt set hostname <name> Sets the hostname of the device. mgmt set nameserver <addr> [<addr2> [<addr3>]] Sets up to three DNS servers for the device. This command overrides any nameservers set through DHCP and any DNS servers previously configured. mgmt set ntp server <server> [<server2> [<server3>]] Sets up to three network time protocol servers for the device. This command overrides any NTP servers set through DHCP and any NTP servers previously configured.

mgmt	<p>mgmt clear nameserver</p> <p>Clears all manually configured DNS servers. Does not change any DNS servers set through DHCP.</p> <p>mgmt clear ntp server</p> <p>Clears all manually configured NTP servers. Does not change any NTP servers set through DHCP.</p>
ping	<p>ping <ip-address> [<size>]</p> <p>Pings from the device to the IP address with the specified sized packets using the MGMT interface. Use CTRL-C to stop.</p>
reboot	<p>reboot</p> <p>Reboots the device. Returns user to the login prompt after reboot.</p>
serialnumber	<p>serialnumber</p> <p>Displays the serial number of the unit.</p>
upgrade	<p>upgrade <upgrade-image-url></p> <p>Upgrades the Netropy firmware. FTP, HTTP, and TFTP services are supported. Ex: upgrade ftp://server/netropy-image</p>
version	<p>version</p> <p>Displays the operating firmware version.</p>

15.3 RADIUS Management Commands

Command	Syntax and Description
show	<p>mgmt show radius</p> <p>Displays the current RADIUS configuration.</p>
set	<p>mgmt set radius server <server></p> <p>Identifies the RADIUS server by IP address or host name. Communication to RADIUS server occurs over the default port 1812. Ex.: mgmt set radius server radiusserver.example.com</p> <p>mgmt set radius secret <secret></p> <p>Set the shared secret that the RADIUS server uses to authorize the client. Ex.: mgmt set radius secret secret_key</p> <p>mgmt set radius { on off }</p> <p>Turns RADIUS authentication on or off.</p>
clear	<p>mgmt clear radius</p> <p>Turns off RADIUS authentication and clears the RADIUS configuration.</p>

15.4 LDAP Management Commands

Command	Syntax and Description
show	<pre>mgmt show radius</pre> <p>Displays the current RADIUS configuration.</p>
set	<pre>mgmt set ldap server <server> [port <#>]</pre> <p>Identifies the LDAP server by IP address or host name. Optionally specifies a non-standard port to connect to. The default port is 389. Ex.: <code>mgmt set ldap server ldapserver.example.com</code></p> <pre>mgmt set ldap basedn <search-base-DN></pre> <p>Identifies the Distinguished Name of the search based in the remote LDAP database. If there are embedded spaces in the base DN string, the string must be enclosed in quotation marks. Ex.: <code>mgmt set ldap basedn dc=example,dc=com</code></p> <pre>mgmt set ldap filter attribute <string> [<LDAP-search-string>]</pre> <p>Specifies the attribute that contains the username and optionally an additional LDAP search string. The LDAP search string must be compatible with the formal definition found in RFC 4515. If there are embedded spaces in the search string, the string must be enclosed in quotation marks. Ex.: <code>mgmt set ldap filter attribute uid & (&(gidNumber=20)(class=Expert))</code> The resulting search string will be <code>(&(uid=user) (&(gidNumber=20) (class=Expert)))</code> where "user" is replaced by the login name.</p> <pre>mgmt set ldap security {disable enable}</pre> <p>Enable or disable Transport Level Security. TLS is enabled by default.</p> <pre>mgmt set ldap bind dn <bind-DN> [password <password>]</pre> <p>Specifies a Distinguished Name and password with which to bind to the LDAP server before performing a search operation. If not configured, an anonymous bind will be used. Ex.: <code>mgmt set ldap bind dn cn=user, dc=example,dc=com</code></p> <pre>mgmt set ldap { on off }</pre> <p>Turns LDAP authentication on or off.</p>
clear	<pre>mgmt clear ldap</pre> <p>Turns off LDAP authentication and clears the LDAP configuration.</p>

16

PROTOCOL GUIDE

This table shows which protocol can or cannot be set under certain packet sizes.

Protocol	64 Bytes	128 Bytes	512 Bytes	1024 Bytes	1500 Bytes
ARP					

NNTP RES

17 SECURITY

17.1 Users and Passwords

Initially, the TrafficEngine system has a single user configured with the following credentials:

- ▶ Username: admin
- ▶ Password: admin

Refer to Section 14 for additional information on proper management and addition of user accounts through the GUI interface.

18 APPOSITE SUPPORT

18.1 Registration

For access to the Netropy Traffic Generator support site with firmware upgrades, documentation, and other support materials, register your unit at: <http://www.apposite-tech.com/register.html>.

Registered users will receive an email notification whenever new firmware versions are released.

18.2 Customer Support

If you experience any problems with the Netropy Traffic Generator hardware, consult the *Hardware Guide* for your intended model. If you have any questions about the firmware that have not been answered in this *User's Guide*, please check the Apposite Technologies website at <http://www.apposite-tech.com> for updated firmware and supporting documentation. If the answer to your inquiry is not answered on the website, please contact Apposite Support.

All units with an active product license may receive support and maintenance for the term of the license. This support includes hardware warranty, firmware updates, and customer support. The license expiration date for limited-term licenses is shown in the Administrative portal of the Netropy Traffic Generator system on the info page.

License renewals are available from Apposite or the reseller of your unit.

If you believe the firmware is not functioning properly, please upgrade to the latest firmware release. If the problem persists, please contact Apposite Support at:

- ▶ support@apposite-tech.com
- ▶ 1.310.477.9955 ext. 2

When contacting Apposite Support, please include the following information with your request:

- ▶ Model number
- ▶ Serial number
- ▶ Your name

- ▶ Your e-mail address and phone number
- ▶ Installed firmware version
- ▶ A detailed description of the problem



Do not attempt to fix any hardware problem yourself. TrafficEngine hardware devices do not contain any user-serviceable parts. Opening the chassis voids the warranty.

APPENDIX A:

APPOSITE END USER LICENSE AGREEMENT

THIS END USER LICENSE AGREEMENT ("AGREEMENT") IS A LEGAL AGREEMENT BETWEEN YOU AND APPOSITE TECHNOLOGIES LLC ("APPOSITE"). BY DOWNLOADING, INSTALLING, COPYING, ACCESSING, OR USING THIS SOFTWARE, YOU AGREE TO THE TERMS OF THIS AGREEMENT. IF YOU ARE ACCEPTING THESE TERMS ON BEHALF OF ANOTHER PERSON OR COMPANY OR OTHER LEGAL ENTITY, YOU REPRESENT AND WARRANT THAT YOU HAVE FULL AUTHORITY TO BIND THAT PERSON, COMPANY, OR LEGAL ENTITY TO THESE TERMS. IF YOU DO NOT AGREE TO THESE TERMS, ARE NOT AT LEAST 18 YEARS OF AGE, OR DO NOT HAVE AUTHORITY TO ENTER THIS AGREEMENT, DO NOT DOWNLOAD, INSTALL, COPY, ACCESS OR USE THIS SOFTWARE, AND PROMPTLY RETURN THIS SOFTWARE AND PROOF OF ENTITLEMENT TO THE PARTY FROM WHOM YOU ACQUIRED THEM.

1. DEFINITIONS.

- a. "Documentation" means published user manuals and other explanatory materials provided by Apposite relating to the Software or the Hardware.
- b. "Hardware" means the Apposite-branded hardware product on which the Software is designed to run.
- c. "Software" means the computer software (regardless of format or media in which distributed) designed to run on the Hardware.
- d. "Modifications" means any applicable upgrades, modified versions, updates, bug fixes, patches, or other modifications to the Software made generally available by Apposite to its customers.
- e. "Product" means the Apposite-branded product comprised of the Hardware, the Software, and the Documentation.
- f. "Legacy Product" means any Product purchased prior to August 1, 2017.
- g. "License Period" means for any Product that is not a Legacy Product, the license period identified on the relevant order form or receipt upon your purchase of the Product or the Software, including any purchased extension thereto.
- h. "Warranty Period" means (a) for any Legacy Product, the period during which you maintain a continuous, active subscription to Apposite maintenance services, or (b) for any Product that is not a Legacy Product, the License Period, unless such Product has a perpetual license, in which case the Warranty Period shall be five (5) years from the date of purchase of the Product from Apposite unless extended by purchase of maintenance services.

2. LICENSE GRANT.

Conditioned upon compliance with the terms and conditions of this Agreement, Apposite hereby grants you the following licenses (collectively, the "License"):

- a. With respect to any Product that is not a Legacy Product, for the relevant License Period, a nonexclusive, nonsublicensable, nontransferable license to use the Software and Modifications solely as embedded in the Hardware, and to use the Documentation solely in conjunction with the Software, Modifications, and Hardware; and
- b. With respect to any Legacy Product, a perpetual, nonexclusive, nonsublicensable, nontransferable license to use the Software solely as embedded in the Hardware, and to use the Documentation solely in conjunction with such Software and Hardware, and to use any Modifications released by Apposite and installed on the Hardware during the Warranty Period.

This license is not a sale. The Software may contain open source or third-party software, subject to separate

license terms. Acknowledgements, licensing terms and disclaimers for such materials are contained in the Documentation, and your use of such material is governed by their respective terms and not by the License.

3. **OWNERSHIP.** Apposite and its licensors retain ownership of all intellectual property rights in and to the Software and Documentation, including any copies, improvements, enhancements, derivative works, and modifications thereof. The Software and Documentation are protected by United States and international copyright and other intellectual property laws and international trade provisions. Your rights to use the Software and Documentation are limited to those expressly granted by this Agreement. No other rights with respect to the Software or any related intellectual property rights are granted or implied.
4. **RESTRICTIONS.** Except as otherwise expressly provided under this Agreement, you shall not directly or authorize any third party to:
 - (i) copy the Software, except as necessary for archival or backup purposes only;
 - (ii) transfer, assign, sublicense, rent, lease, lend, or otherwise transfer your license rights to any other person or entity;
 - (iii) install or use the Software on any computing device other than the Hardware;
 - (iv) modify or adapt the Software or Documentation or create derivative works based upon the Software or Documentation;
 - (v) reverse engineer, disassemble, decompile, decrypt, or otherwise attempt to derive the source code of the Software, except to the extent otherwise expressly permitted under applicable law notwithstanding this restriction; or
 - (vi) remove, alter, cover, or obfuscate any of the trademarks, trade names, logos, patent or copyright notices or markings, or add any other notices or markings to or on the Software, Documentation, or Hardware without the express written authorization of Apposite.
5. **SUPPORT.** Apposite shall have no obligation to support the Software except as provided in Apposite's Customer Support Terms and Conditions, which is incorporated by reference into this Agreement.
6. **LIMITED WARRANTY.** Apposite warrants that, for the duration of the Warranty Period, the Hardware will be free of any defects in materials and workmanship under normal use and the Software will perform substantially in accordance with the Documentation. This limited warranty extends only to the original user of the Product. This limited warranty is void if failure of the Hardware or Software to conform to the warranty has resulted from improper installation, testing, misuse, neglect, accident, fire or other hazard, a virus, or any breach of this Agreement. Apposite and its suppliers' entire liability and your sole and exclusive remedy shall be, at Apposite's sole discretion, to: (i) repair the Software or Hardware; (ii) provide replacement Hardware or Software; or (iii) refund the purchase price and terminate this Agreement. This limited warranty applies only if the Product is returned to Apposite, freight and insurance prepaid, in accordance with Apposite's Return Material Authorization (RMA) procedures. Any repaired or replaced Software or Hardware will be subject to this same limited warranty for the remainder of the original Warranty Period or thirty (30) days, whichever is greater. THE FOREGOING LIMITED WARRANTY IS IN LIEU OF ALL OTHER WARRANTIES OR CONDITIONS, EXPRESS OR IMPLIED, AND APPOSITE DISCLAIMS ANY AND ALL IMPLIED WARRANTIES OR CONDITIONS, INCLUDING, WITHOUT LIMITATION, ANY IMPLIED WARRANTY OF TITLE, NONINFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. THIS WARRANTY GIVES YOU SPECIFIC LEGAL RIGHTS, AND YOU MAY ALSO HAVE OTHER RIGHTS WHICH VARY BY JURISDICTION.
7. **LIMITATION OF LIABILITY.** REGARDLESS WHETHER ANY REMEDY SET FORTH HEREIN FAILS OF ITS ESSENTIAL PURPOSE, IN NO EVENT WILL APPOSITE OR ITS SUPPLIERS BE LIABLE FOR ANY DAMAGES,

INCLUDING WITHOUT LIMITATION, ANY LOST PROFITS, BUSINESS INTERRUPTION, LOSS OF INFORMATION, OR OTHER INCIDENTAL OR CONSEQUENTIAL DAMAGES HOWEVER CAUSED AND REGARDLESS OF THE THEORY OF LIABILITY OR WHETHER ARISING OUT OF THE USE OF OR INABILITY TO USE THE PRODUCT AND EVEN IF APPOSITE OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. IN NO EVENT SHALL APPOSITE OR ITS SUPPLIERS' LIABILITY, WHETHER IN CONTRACT, TORT (INCLUDING NEGLIGENCE), BREACH OF WARRANTY, OR OTHERWISE, EXCEED THE PRICE PAID FOR THE PRODUCT. SOME STATES DO NOT ALLOW THE LIMITATION OR EXCLUSION OF LIABILITY FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES, SO THE ABOVE LIMITATION MAY NOT APPLY TO YOU. YOU HEREBY WAIVE CALIFORNIA CIVIL CODE SECTION 1542, WHICH SAYS "A GENERAL RELEASE DOES NOT EXTEND TO CLAIMS WHICH THE CREDITOR DOES NOT KNOW OR SUSPECT TO EXIST IN HIS FAVOR AT THE TIME OF EXECUTING THE RELEASE, WHICH, IF KNOWN BY HIM MUST HAVE MATERIALLY AFFECTED HIS SETTLEMENT WITH THE DEBTOR."

8. **TERM AND TERMINATION.** This Agreement takes effect upon your use of the Software and remains effective until terminated. You may terminate it at any time by destroying all copies of the Software and Documentation in your possession. The licenses granted by Apposite herein will terminate immediately if you fail to comply with any term or condition of this Agreement. You agree on termination of the licenses to cease all use of the Software and Documentation. In addition, the provisions of the sections "U.S. Government Restricted Rights" and "Export" shall survive termination of this Agreement.
9. **EXPORT.** The Product, including the underlying technology, is subject to U.S. export control laws, and may be subject to export or import regulations in other countries. You may not export or import the Product and the underlying technology, directly or indirectly, in violation of these laws. You agree to comply strictly with all such laws and regulations and acknowledge that you have the responsibility to obtain such licenses to export, re-export, or import as may be required.
10. **U.S. GOVERNMENT RESTRICTED RIGHTS.** All Software and Documentation provided pursuant to this Agreement qualifies as "commercial computer software" and "commercial computer software documentation" pursuant to FAR 12.212 and DFAR 227.7202. The Software and Documentation are being licensed to U.S. Government end users only as commercial items and with only those rights as are granted to all other end users pursuant to the terms and conditions of this agreement.
11. **GENERAL PROVISIONS.** This Agreement will be governed by and construed in accordance with the laws of the State of California without reference to its conflicts of law provisions. Any dispute arising out of or relating to this Agreement shall be subject to the exclusive jurisdiction and venue of the courts sitting in Los Angeles, California. This Agreement shall not be governed by either the Uniform Computer Information Transactions Act (UCITA) or the United Nations Convention on Contracts for the International Sale of Goods (CISG), the application of which is expressly excluded. If for any reason a court of competent jurisdiction finds any provision of this Agreement, or any portion thereof, to be unenforceable, the remainder of this Agreement shall continue in full force and effect. This Agreement constitutes the entire agreement between the parties with respect to the Product and supersedes all prior or contemporaneous understandings regarding such subject matter, whether written or oral, and supersedes any conflicting or additional terms contained in any purchase order or elsewhere, all of which terms are excluded. No amendment to or modification of this Agreement are binding unless in writing and signed by Apposite.

Apposite® Technologies LLC

4223 Glencoe Ave, Suite B121

Marina Del Rey, CA 90292 USA

1.310.477.9955

info@apposite-tech.com

www.apposite-tech.com