Quick Reference
Guide

IxNetwork WebUI

KEYSIGHT
TECHNOLOGIES

Notices

Warranty

THE MATERIAL CONTAINED IN THIS DOCUMENT IS PROVIDED "AS IS," AND IS SUBJECT TO BEING CHANGED, WITHOUT NOTICE, IN FUTURE EDITIONS. FURTHER, TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, KEYSIGHT DISCLAIMS ALL WARRANTIES, EITHER EXPRESS OR IMPLIED WITH REGARD TO THIS MANUAL AND ANY INFORMATION CONTAINED HEREIN, INCLUDING BUT NOT LIMITED TO THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. KEYSIGHT SHALL NOT BE LIABLE FOR ERRORS OR FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES IN CONNECTION WITH THE FURNISHING, USE, OR PERFORMANCE OF THIS DOCUMENT OR ANY INFORMATION CONTAINED HEREIN. SHOULD KEYSIGHT AND THE USER HAVE A SEPARATE WRITTEN AGREEMENT WITH WARRANTY TERMS COVERING THE MATERIAL IN THIS DOCUMENT THAT CONFLICT WITH THESE TERMS, THE WARRANTY TERMS IN THE SEPARATE AGREEMENT WILL CONTROL.

Statement of Compliance.

This product has been designed and tested in accordance with accepted industry standards, and has been supplied in a safe condition. The documentation contains information and warnings that must be followed by the user to ensure safe operation and to maintain the product in a safe condition.

Technology Licenses

The hardware and/or software described in this document are furnished under a license and may be used or copied only in accordance with the terms of such license.

Restricted Rights Legend

If software is for use in the performance of a U.S. Government prime contract or subcontract, Software is delivered and licensed as "Commercial computer software" as defined in DFAR 252.227-7014 (June 1995), or as a "commercial item" as defined in FAR 2.101(a) or as "Restricted computer software" as defined in FAR 52.227-19 (June 1987) or any equivalent agency regulation or contract clause. Use, duplication or disclosure of Software is subject to Keysight Technologies' standard commercial license terms, and non-DOD Departments and Agencies of the U.S. Government will receive no greater than Restricted Rights as defined in FAR 52.227-19(c)(1-2) (June 1987). U.S. Government users will receive no greater than Limited Rights as defined in FAR 52.227-14 (June 1987) or DFAR 252.227-7015 (b)(2) (November 1995), as applicable in any technical data.

Safety Notices

The following general safety precautions must be observed during all phases of operation of this instrument. Failure to comply with these precautions or with specific warnings elsewhere in this manual violates safety standards of design, manufacture, and intended use of the instrument. Keysight Technologies Inc. assumes no liability for the customer's failure to comply with these requirements.

CAUTION

A CAUTION notice denotes a hazard. It calls attention to an operating procedure, practice, or the like that, if not correctly performed or adhered to, could result in damage to the product or loss of important data. Do not proceed beyond a CAUTION notice until the indicated conditions are fully understood and met.

WARNING

A WARNING notice denotes a hazard. It calls attention to an operating procedure, practice, or the like that, if not correctly performed or adhered to, could result in personal injury or death. Do not proceed beyond a WARNING notice until the indicated conditions are fully understood and met.

Table of Contents

1. Overview

This reference guide describes the IxNetwork Web application and its usage. It helps IxNetwork test Engineers to configure Ixia test equipment with minimal efforts.

1.1. Introduction to IxNetwork

- IxNetwork is a comprehensive network infrastructure performance testing solution. It scales to handle powerful devices and very large networks, from routing and switching to data center ethernet and software defined networking.
- IxNetwork is specifically targeted for the performance and functionality testing of high-speed, high-capacity routers, switches and other network infrastructure elements.
- Provides a powerful, yet easy-to-use, graphical user interface (GUI) that you can use to configure and run complex tests. The user interface comes in two varieties; a windows based application and a web based application. It is the web app that is the focus of this document.
- Offers the flexibility to customize the configuration settings to meet a wide range of requirements for testing complex network topologies, consisting of thousands of routing or switching devices.
- IxNetwork is capable of emulating millions of routes and addressable hosts within a single topology. It provides the ability to customize millions of traffic flows using the emulated hosts to stress the data plane performance.
- Creates sophisticated configurations using powerful wizards and grid controls in the UI.
- Capable of reporting comprehensive protocol status and detailed per-flow traffic performance metrics based on a wide array of tracking options.

1.2. What is IxNetwork Web App

- IxNetwork Web App is a web-based client UI for Ixia’s layer 2-3 traffic generation test application, and is most commonly used for testing routing and switching networks.
- IxNetwork Web App supports multiple concurrent users and sessions, and allows multiple users to access a session, or a user to access multiple sessions simultaneously.
- IxNetwork Web App has built-in REST API browser that helps users configure the test tool through a UI and then correlate the change directly to REST commands.

1.3. Prerequisites

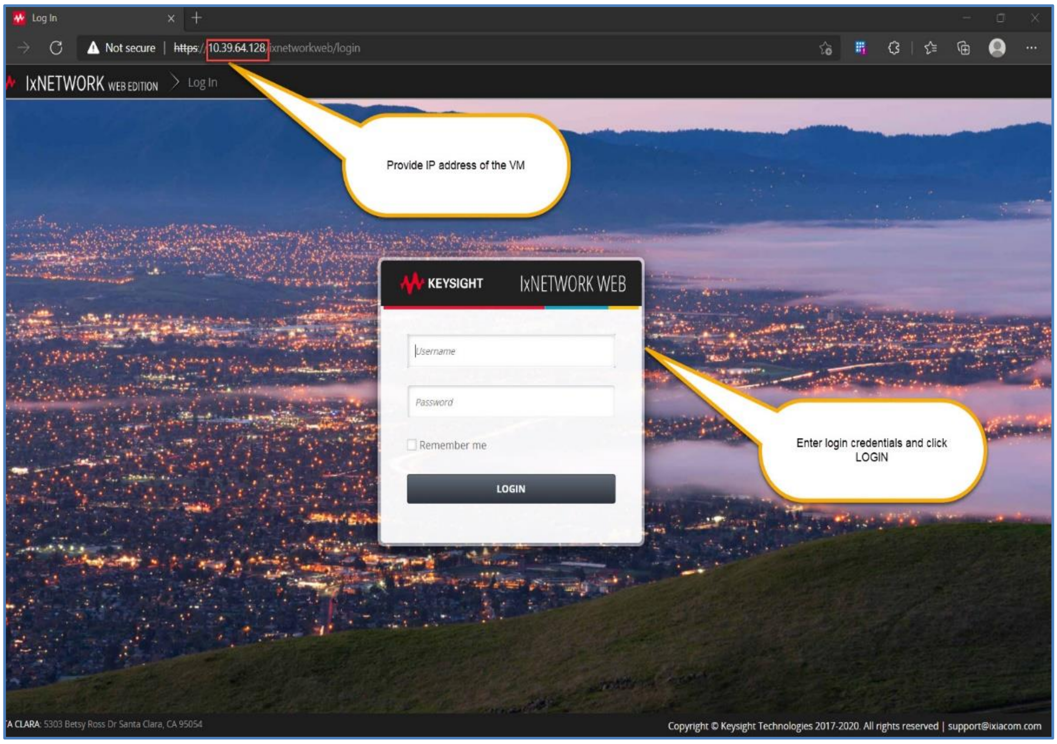
- IxNetwork Version should be 9.00 and above.

2. Configure BGP from the sample scenarios

This section demonstrates creating a BGP test scenario from sample scenarios.

2.1. IxNetwork Web App login

- Provide IP address of the VM or Chassis in the URL.
- Enter login credentials and click LOGIN .



Not secure | https://10.39.64.128/ixnetworkweb/login

Provide IP address of the VM

Enter login credentials and click LOGIN

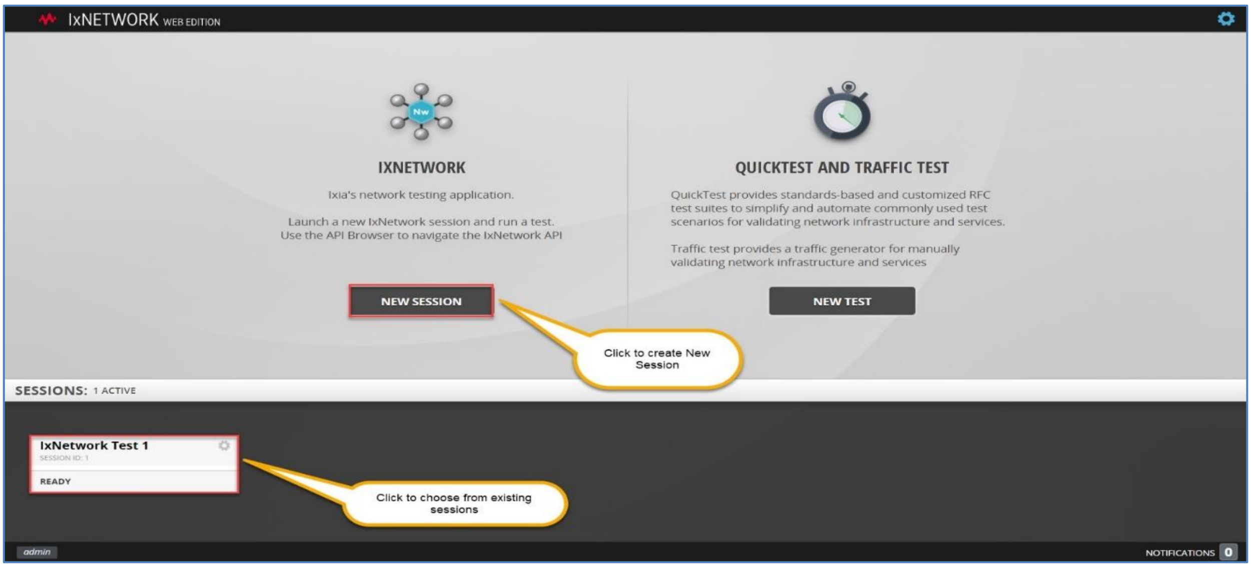
A CLARA: 5303 Betsy Ross Dr Santa Clara, CA 95054

Copyright © Keysight Technologies 2017-2020. All rights reserved | support@ixiacom.com

Fig 2.1-Login page

2.2. Create Session

- Web App allows user to work with multiple sessions by creating a new session or selecting from the existing sessions.



IXNETWORK

Ixia's network testing application.

Launch a new IxNetwork session and run a test.
Use the API Browser to navigate the IxNetwork API

QUICKTEST AND TRAFFIC TEST

QuickTest provides standards-based and customized RFC test suites to simplify and automate commonly used test scenarios for validating network infrastructure and services.

Traffic test provides a traffic generator for manually validating network infrastructure and services

Click to create New Session

SESSIONS: 1 ACTIVE

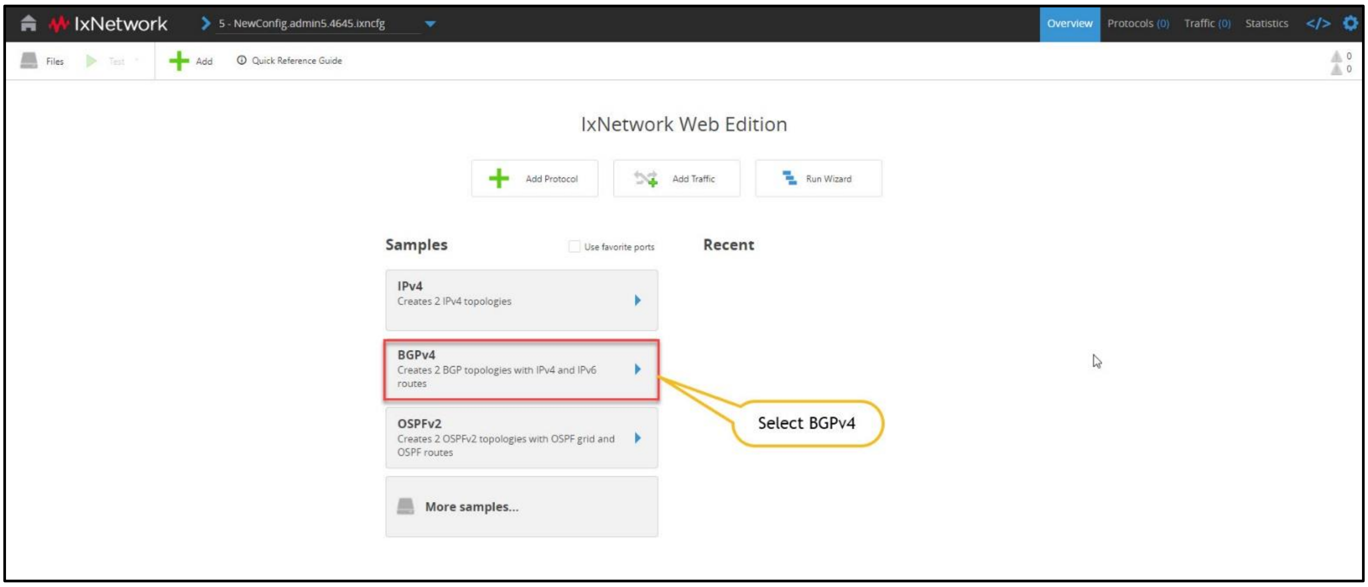
IxNetwork Test 1
SESSION ID: 1
READY

Click to choose from existing sessions

Fig 2.2 Create session window

2.3. Select sample scenario

- ➢ User can choose the test scenarios from the sample or recent scenarios.

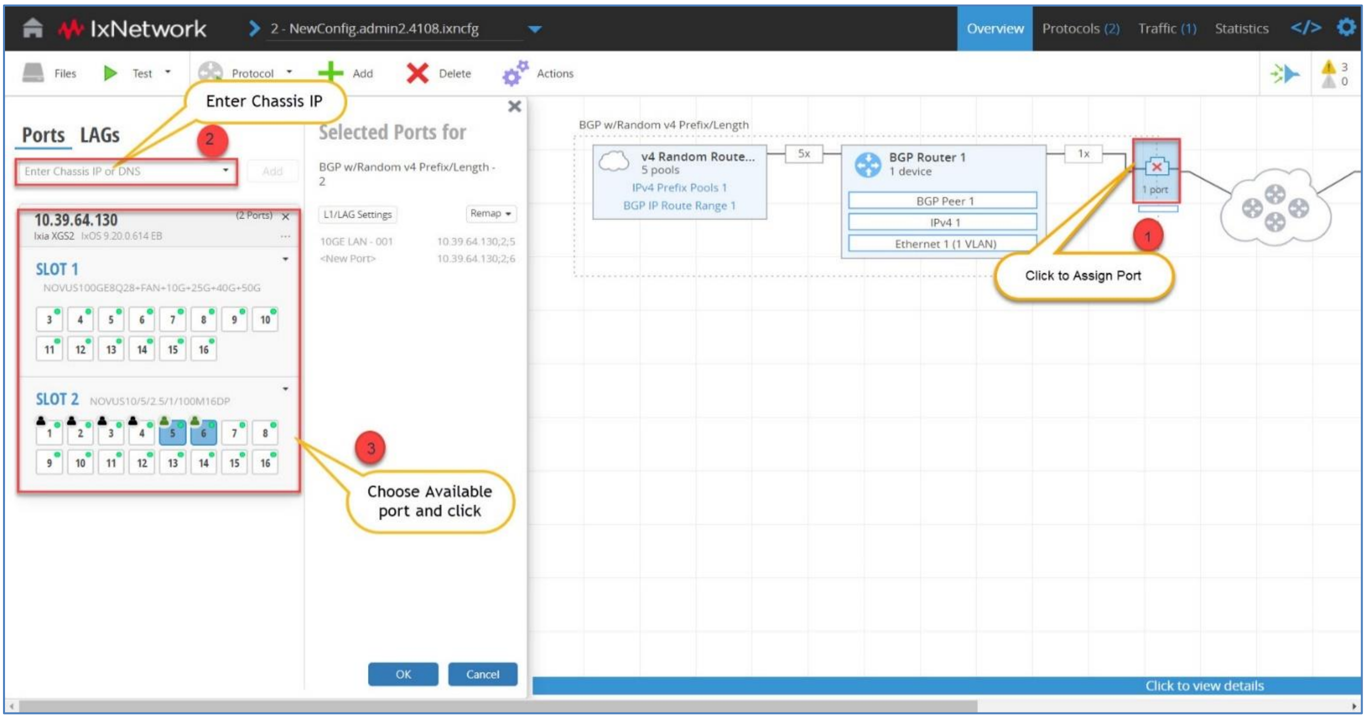


Select BGPv4

Fig 2.3 Select sample scenario

2.4. Assign Ports

- ➢ **Select Ports** window allows user to assign port to the topology, Enter chassis IP and choose the available port from the list of ports, different port states are explained in Fig 2.4.2.
- ➢ User can perform **Select/Unselect**, **Unassign selected ports** and **Remove selected ports** as shown in Fig 2.4.3.
- ➢ User can edit **L1 Settings** as shown in Fig 2.4.4.



Enter Chassis IP

2

Click to Assign Port

1

3

Choose Available port and click

Fig 2.4.1 Assigning and connecting Port

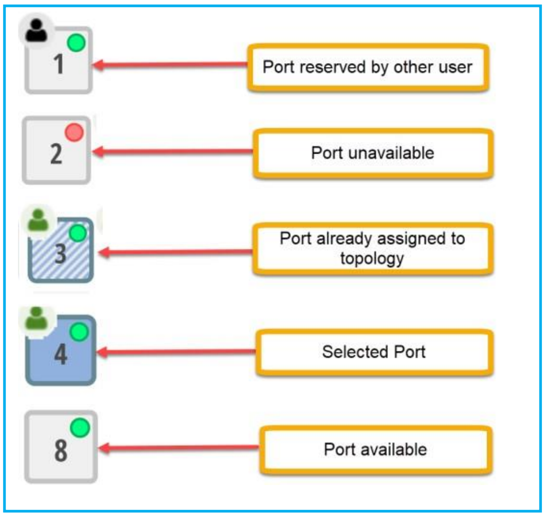
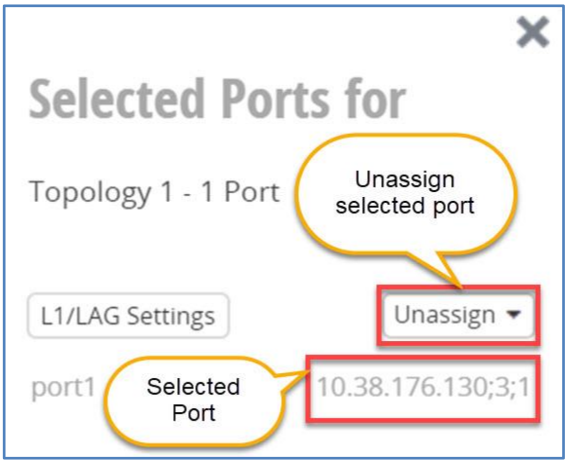

1
Port reserved by other user
2
Port unavailable
3
Port already assigned to topology
4
Selected Port
8
Port available

Fig 2.4.2 Different port states



Selected Ports for

Topology 1 - 1 Port

Unassign selected port

L1/LAG Settings

Unassign ▾

port1

Selected Port

10.38.176.130;3;1

Fig 2.4.3 Port unassign options

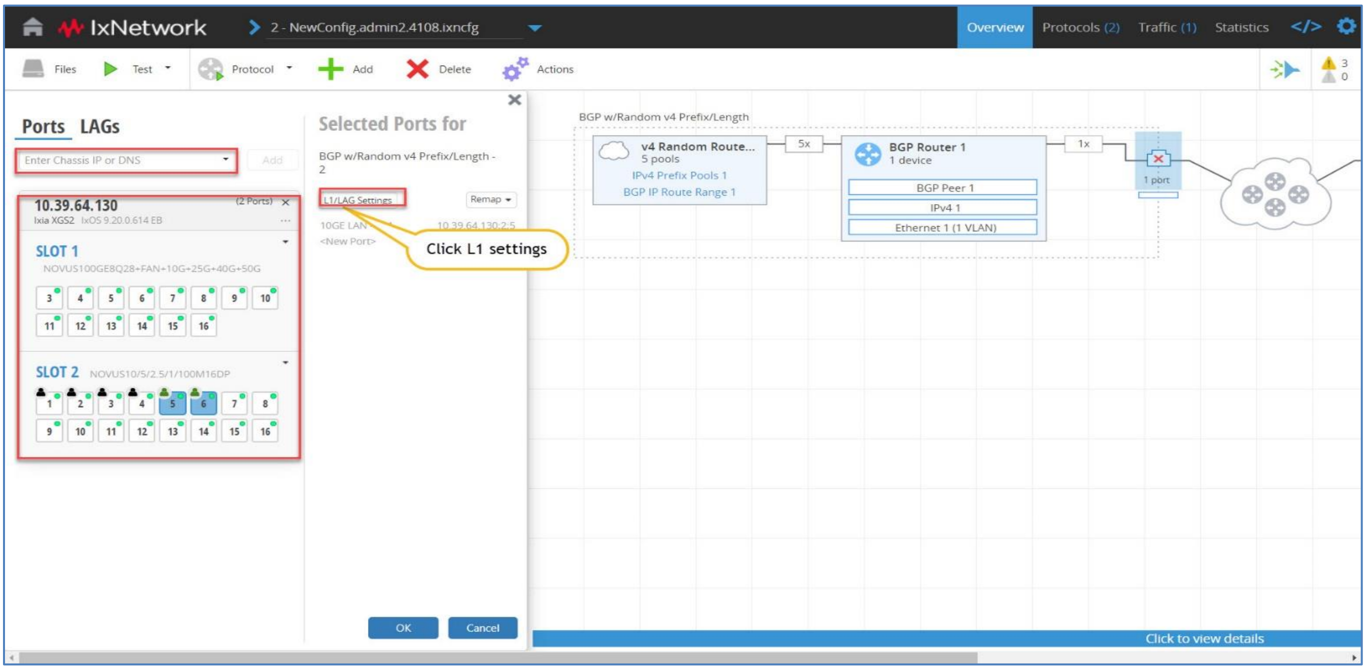
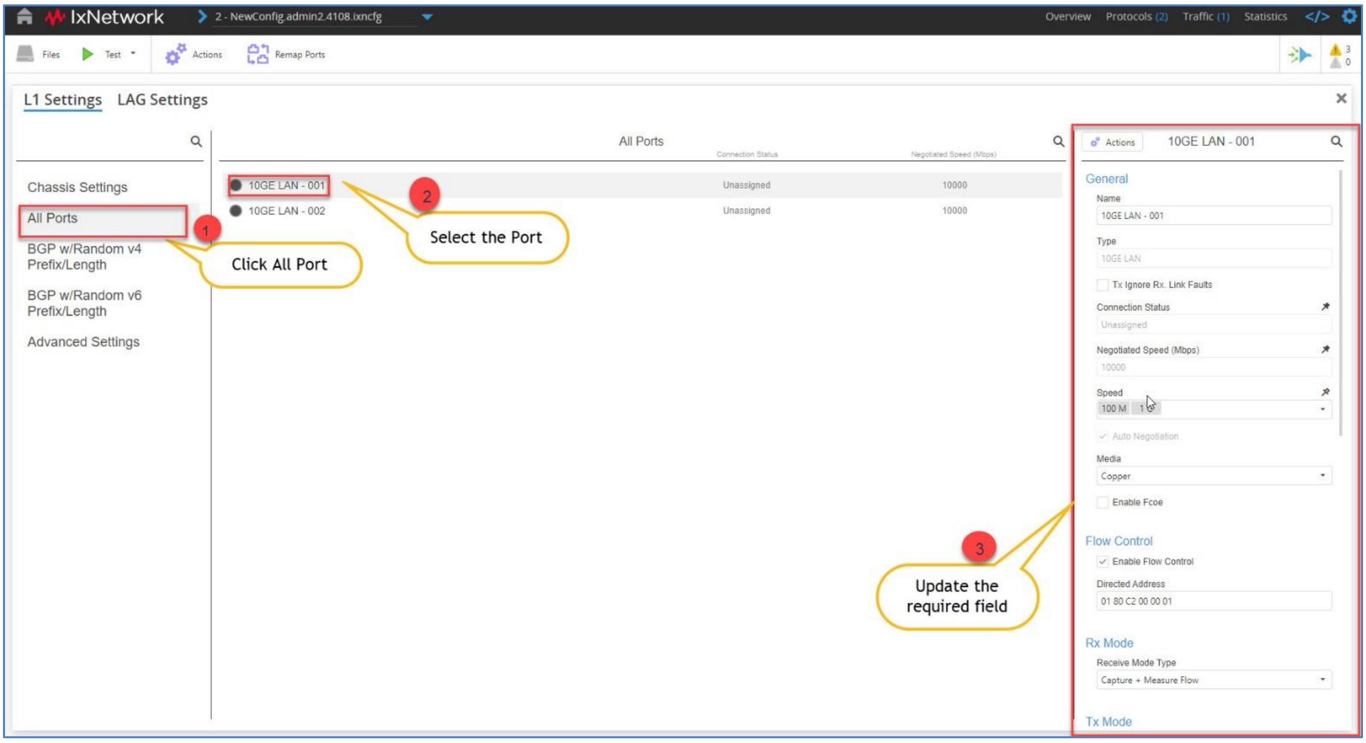


Fig 2.4.4.1 L1 Settings



	Connection Status	Negotiated Speed (Mbps)
10GE LAN - 001	Unassigned	10000
10GE LAN - 002	Unassigned	10000

10GE LAN - 001

General

Name: 10GE LAN - 001

Type: 10GE LAN

□ Tx Ignore Rx. Link Faults

Connection Status: Unassigned

Negotiated Speed (Mbps): 10000

Speed: 100 M 1

✓ Auto Negotiation

Media: Copper

□ Enable Fcoe

Flow Control

☑ Enable Flow Control

Directed Address: 01 80 C2 00 00 01

Rx Mode

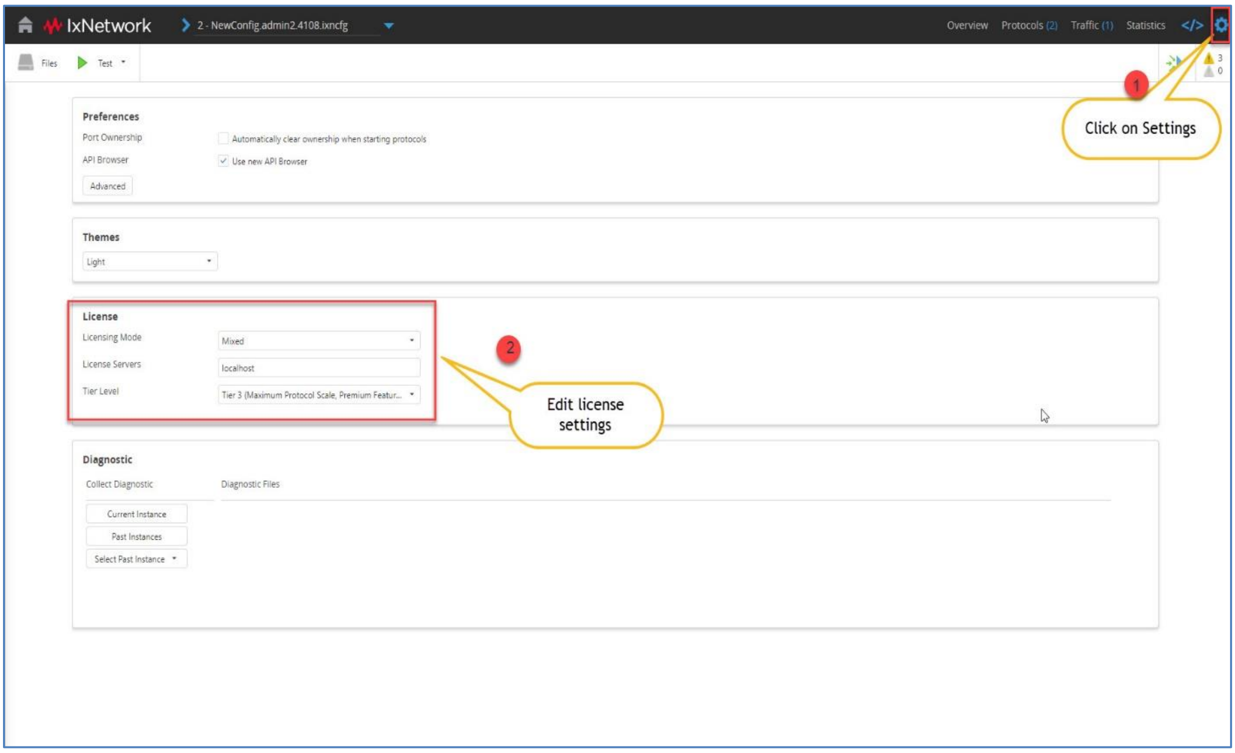
Receive Mode Type: Capture + Measure Flow

Tx Mode

Fig. 2.4.4.2 L1 settings

2.5. License Settings:

- ➢ User can edit License settings from **Settings** page.



Preferences

Port Ownership: □ Automatically clear ownership when starting protocols

API Browser: ☑ Use new API Browser

Themes: Light

License

Licensing Mode: Mixed

License Servers: localhost

Tier Level: Tier 3 (Maximum Protocol Scale, Premium Featur...

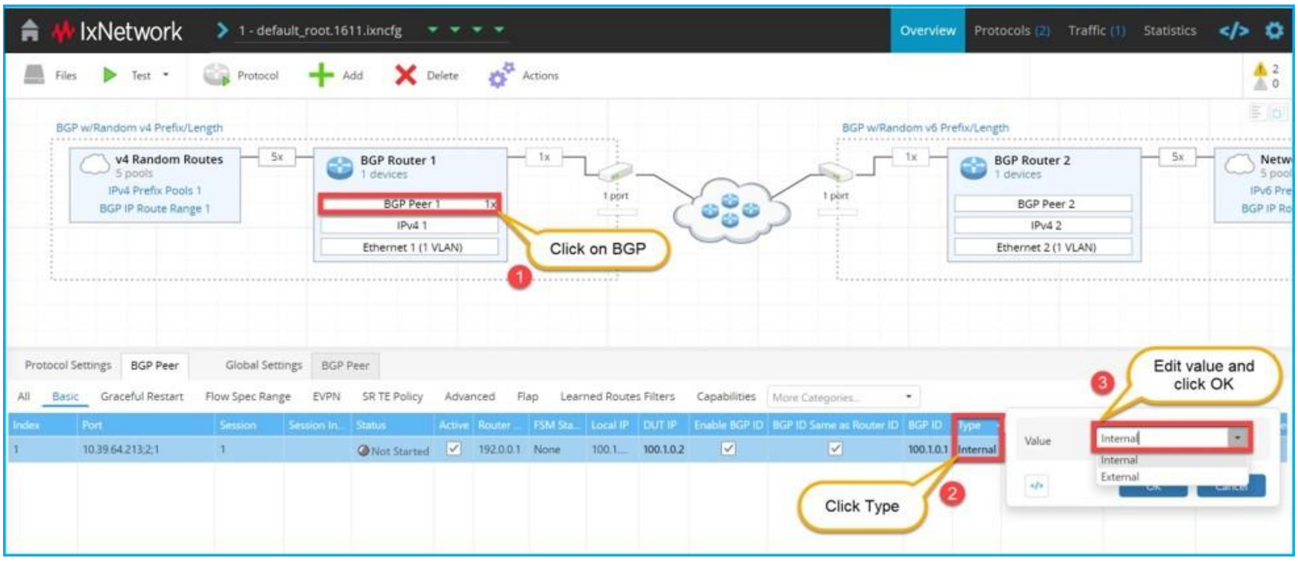
Diagnostic

Collect Diagnostic: Diagnostic Files

Fig 2.5 License Settings

2.6. Edit Protocol grid

- ➢ Edit the required fields from the BGP protocol grid and save the configuration
- ➢ For example, change the BGP Type as shown in Fig 2.6



Index	Port	Session	Session In...	Status	Active	Router ...	FSM Sta...	Local IP	DUT IP	Enable BGP ID	BGP ID Same as Router ID	BGP ID	Type
1	10.39.64.213;2;1	1		Not Started	☑	192.0.0.1	None	100.1....	100.1.0.2	☑	☑	100.1.0.1	Internal

Fig 2.6 Edit BGP Protocol grid

2.7. Run Test/Protocol

- Run the Test scenario by clicking on **Test** or **Protocol**.
- As shown in Fig 2.7.2, observe the ports getting connected and all the protocols getting started, followed by Traffic.

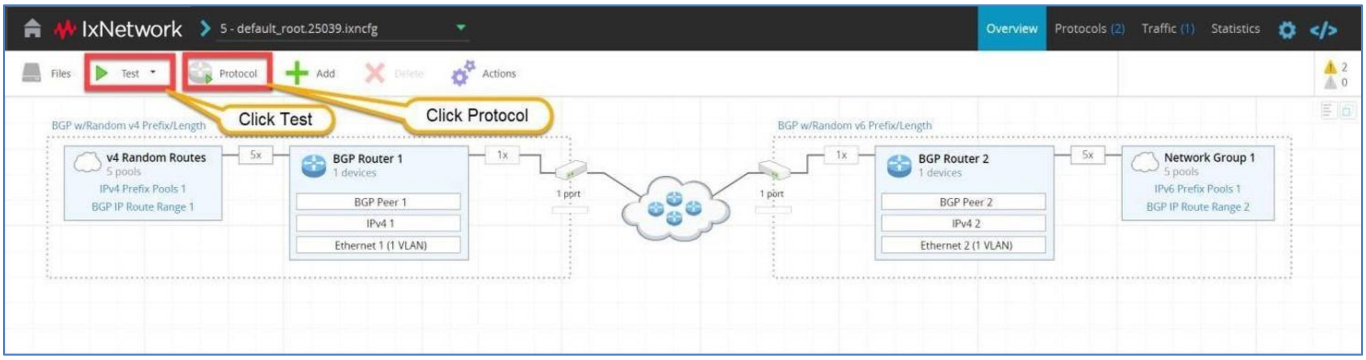


Fig 2.7.1 Run Test/Protocol

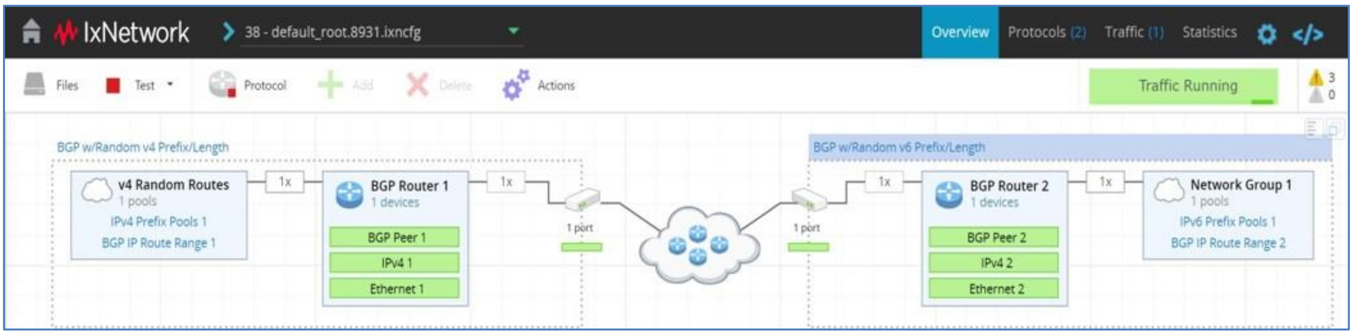
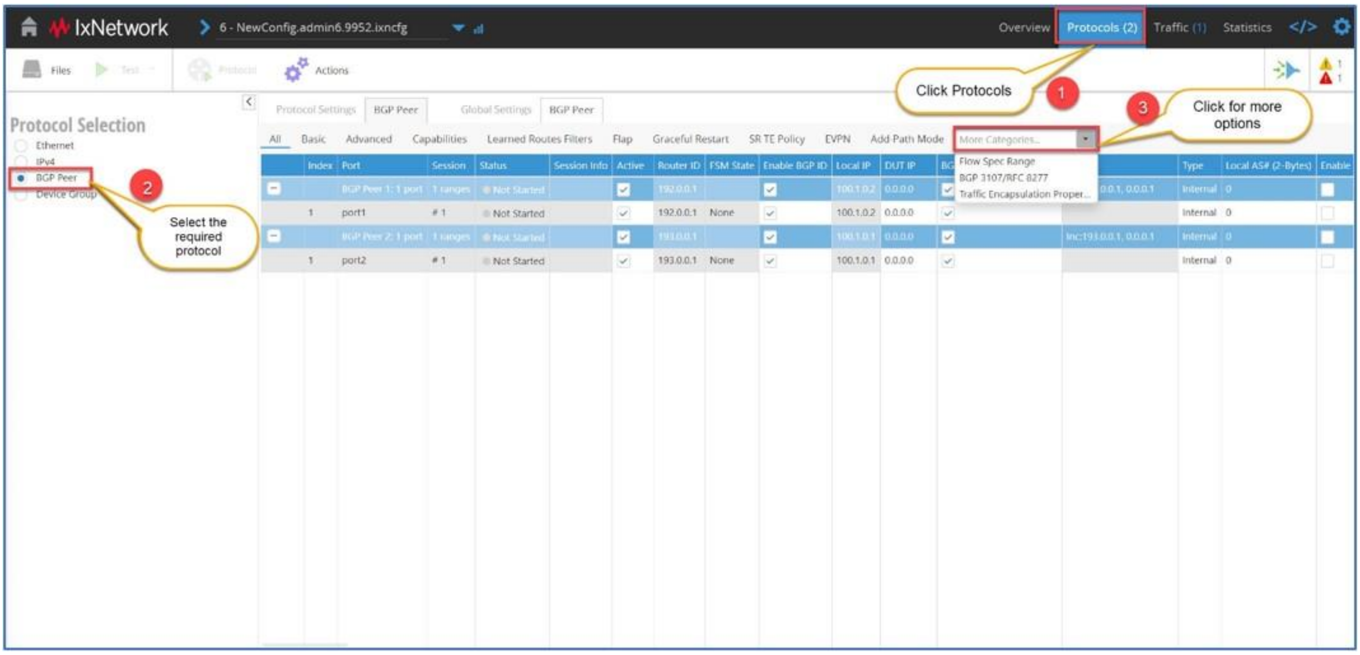


Fig 2.7.2 Protocol Status after run Test

2.8. Protocol View

- User can view the details of the protocol in **Protocols** page.
- User can choose different view options from the drop down list.



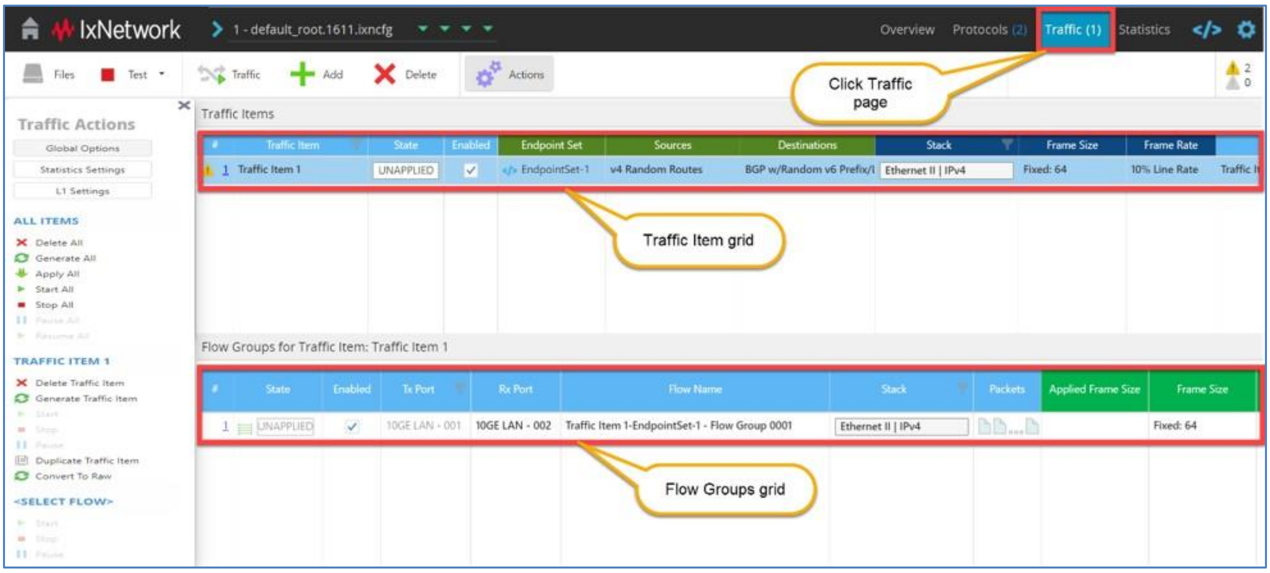
	Index	Port	Session	Status	Session Info	Active	Router ID	FSM State	Enable BGP ID	Local IP	DUT IP	BG		Type	Local AS# (2-Bytes)	Enable
−		BGP Peer 1: 1 port	1 ranges	Not Started		✓	192.0.0.1		✓	100.1.0.2	0.0.0.0	✓	0.0.1, 0.0.0.1	Internal	0	□
	1	port1	# 1	Not Started		✓	192.0.0.1	None	✓	100.1.0.2	0.0.0.0	✓		Internal	0	□
−		BGP Peer 2: 1 port	1 ranges	Not Started		✓	193.0.0.1		✓	100.1.0.1	0.0.0.0	✓	Inc:193.0.0.1, 0.0.0.1	Internal	0	□
	1	port2	# 1	Not Started		✓	193.0.0.1	None	✓	100.1.0.1	0.0.0.0	✓		Internal	0	□

Fig 2.8 Protocol View

2.9. Traffic Grid

- **Traffic item** and **flow groups** grids are interactive, user can edit the fields and save the configuration which is shown in detail in section 3.10.
- Create the flow groups based on the selectable packet fields, osne flow group/high-level stream is created for each selected field.

*Editing the traffic item and setting up the flow group is optional



Traffic Items

#	Traffic Item	State	Enabled	Endpoint Set	Sources	Destinations	Stack	Frame Size	Frame Rate	
1	Traffic Item 1	UNAPPLIED	✓	EndpointSet-1	v4 Random Routes	BGP w/Random v6 Prefix/I	Ethernet II | IPv4	Fixed: 64	10% Line Rate	Traffic I

Flow Groups for Traffic Item: Traffic Item 1

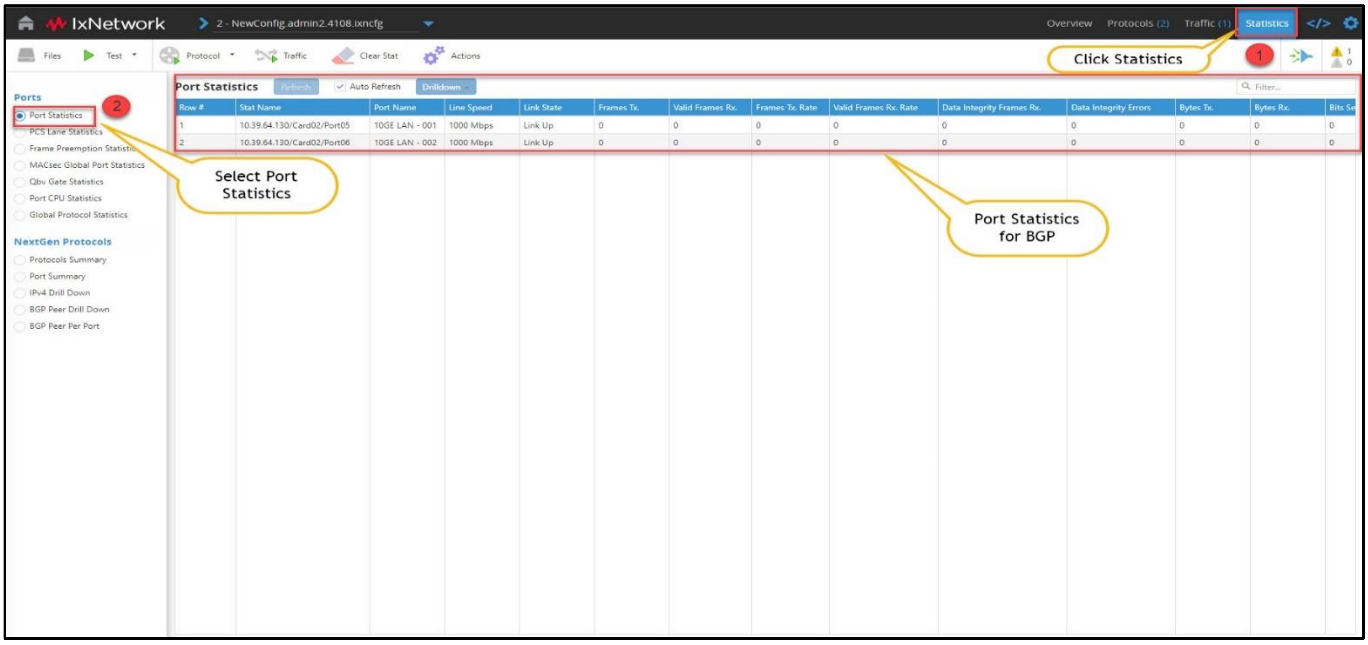
#	State	Enabled	Tx Port	Rx Port	Flow Name	Stack	Packets	Applied Frame Size	Frame Size
1	UNAPPLIED	✓	10GE LAN - 001	10GE LAN - 002	Traffic Item 1-EndpointSet-1 - Flow Group 0001	Ethernet II | IPv4			Fixed: 64

Fig 2.9 Traffic Grid

2.10. Statistics View

- User can view the traffic statistics from the **Statistics** page.
- User can view different statistics like **Port Statistics**, traffic **Flow Statistics** and traffic

dashboard as shown in the Figures 2.10.1, 2.10.2 and 2.10.3.



Click Statistics

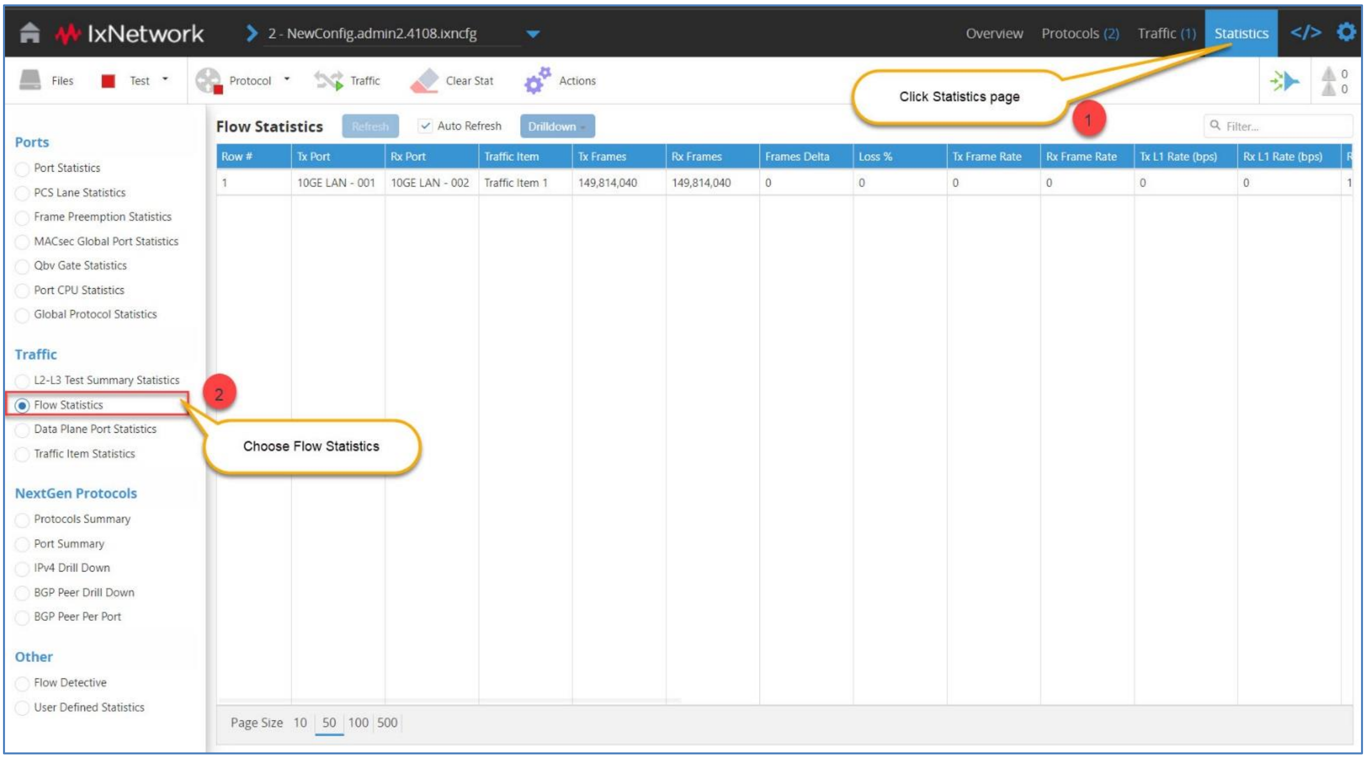
Select Port Statistics

Port Statistics for BGP

Port Statistics ☑ Auto Refresh

Row #	Stat Name	Port Name	Line Speed	Link State	Frames Tx.	Valid Frames Rx.	Frames Tx. Rate	Valid Frames Rx. Rate	Data Integrity Frames Rx.	Data Integrity Errors	Bytes Tx.	Bytes Rx.	Bits Se
1	10.39.64.130/Card02/Port05	10GE LAN - 001	1000 Mbps	Link Up	0	0	0	0	0	0	0	0	0
2	10.39.64.130/Card02/Port06	10GE LAN - 002	1000 Mbps	Link Up	0	0	0	0	0	0	0	0	0

Fig 2.10.1 Port Statistics View



Click Statistics page

Choose Flow Statistics

Flow Statistics ☑ Auto Refresh

Row #	Tx Port	Rx Port	Traffic Item	Tx Frames	Rx Frames	Frames Delta	Loss %	Tx Frame Rate	Rx Frame Rate	Tx L1 Rate (bps)	Rx L1 Rate (bps)	R
1	10GE LAN - 001	10GE LAN - 002	Traffic Item 1	149,814,040	149,814,040	0	0	0	0	0	0	1

Fig 2.10.2 Traffic Flow Statistics View

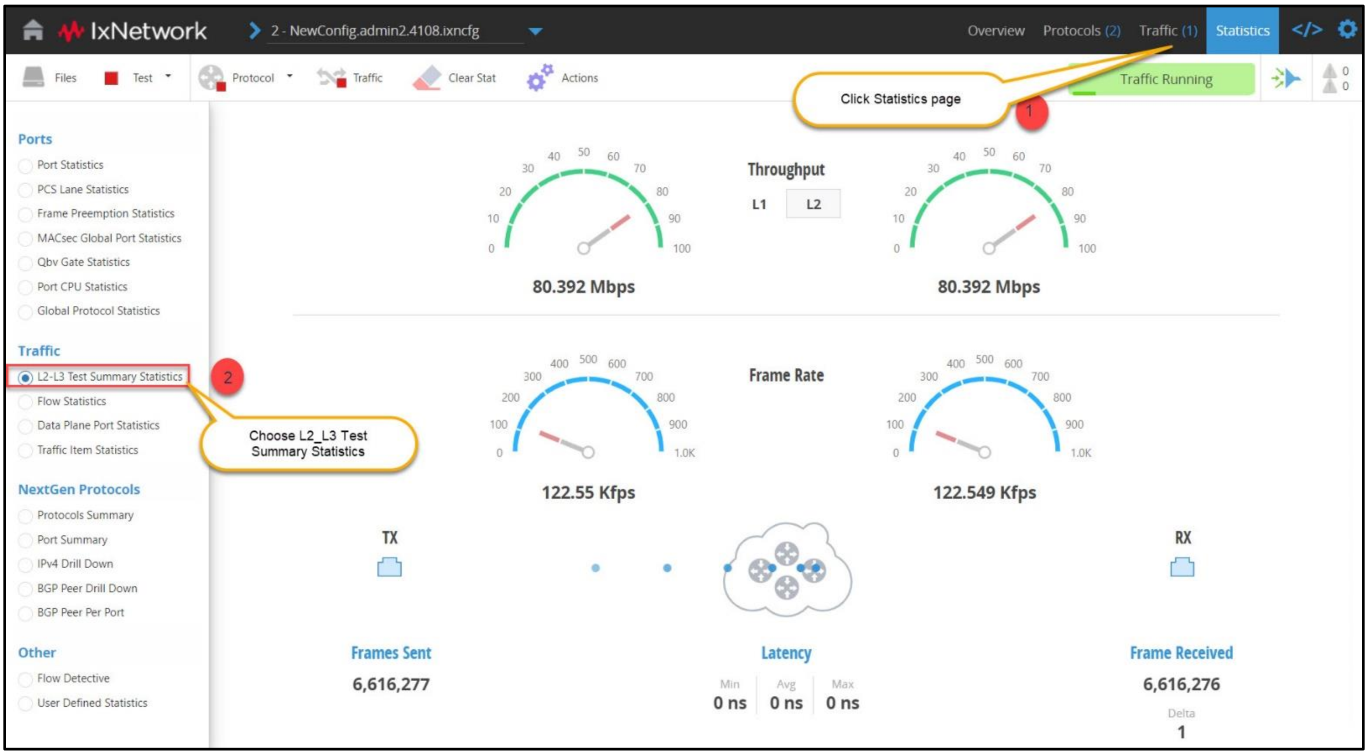


Fig 2.10.3 L2/L3 Traffic Dashboard

3. Configure OSPF from scratch

This section walks through a scenario which configures OSPF emulation manually to get the user introduced to most of the basic features of Web App.

3.1. Add Test Scenario

- User can add a new test scenario by clicking **Add** from the Overview page.
- User can also choose an existing scenario from samples or recent list of scenarios.

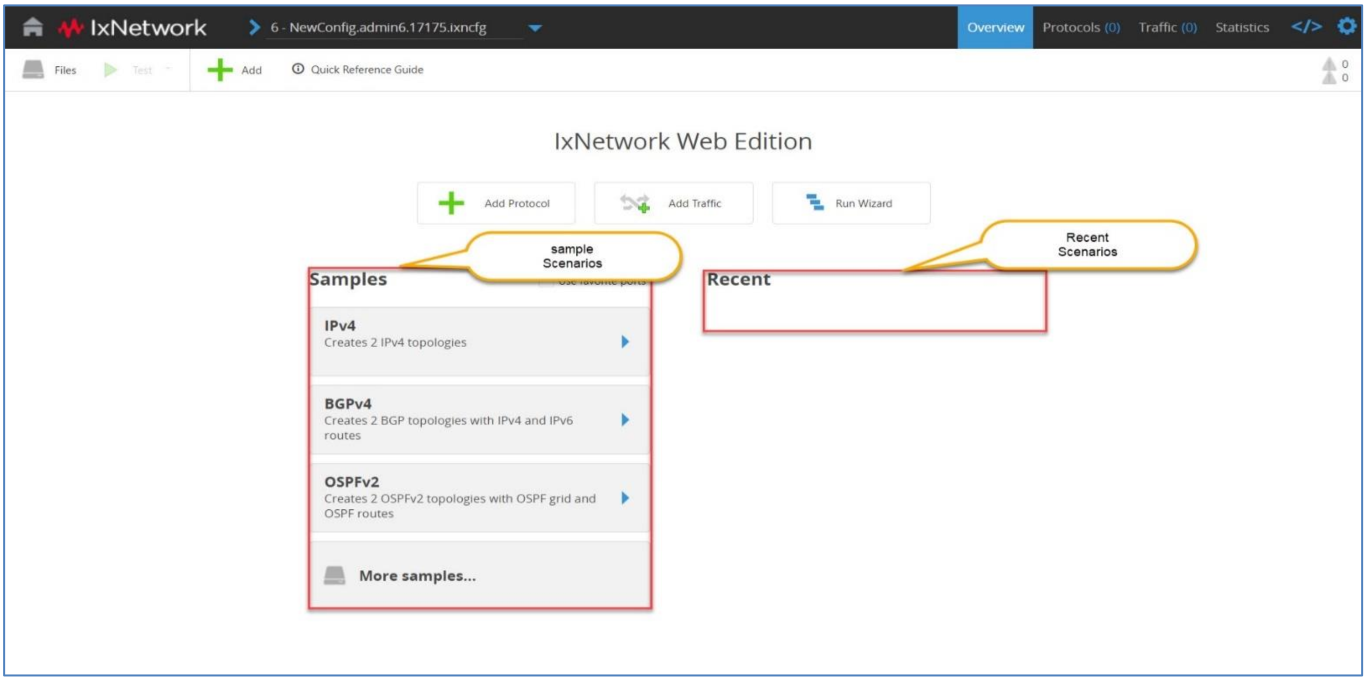
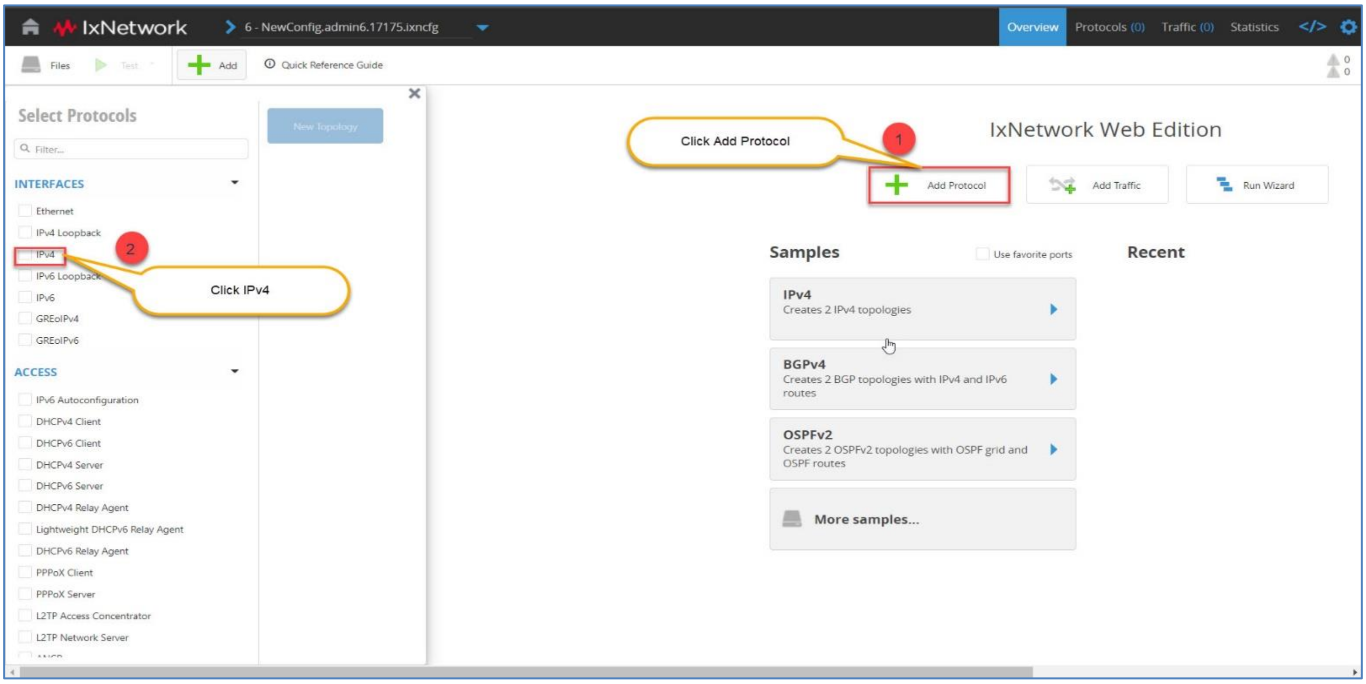


Fig 3.1 Overview page-Create Test scenario

3.2. Select Protocol

- The **Select Protocols** window allows user to select protocol from the list of supported protocols, for example IPv4.
- Scroll down to view all the available protocols.



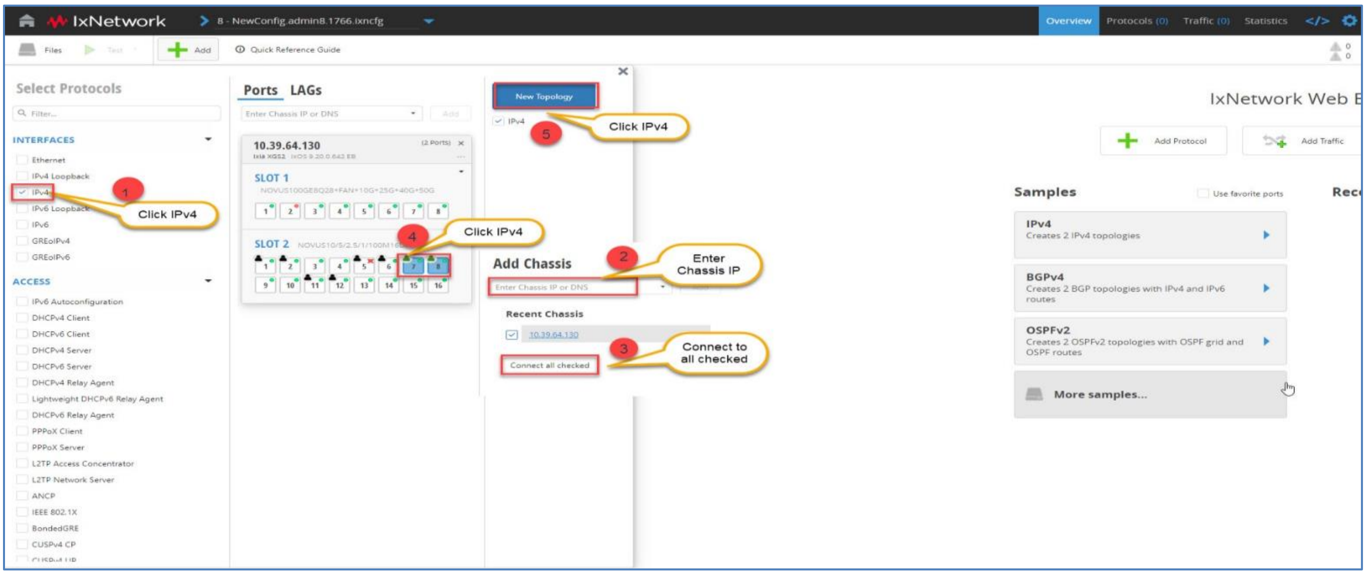
1 Click Add Protocol

2 Click IPv4

Fig 3.2 Select Protocol

3.3. Add Chassis and Port

- The Port selection window allows user to manage ports.
- After choosing a protocol from the list, **Add Chassis** window pops up to the user, select chassis by entering chassis IP or select chassis from the list of recently used chassis and click **Connect all checked**.
- Select the available port under the chassis in **Select Ports** window and click **New Topology.**
- User can add multiple topologies before closing the topology window.



1 Click IPv4

2 Enter Chassis IP

3 Connect to all checked

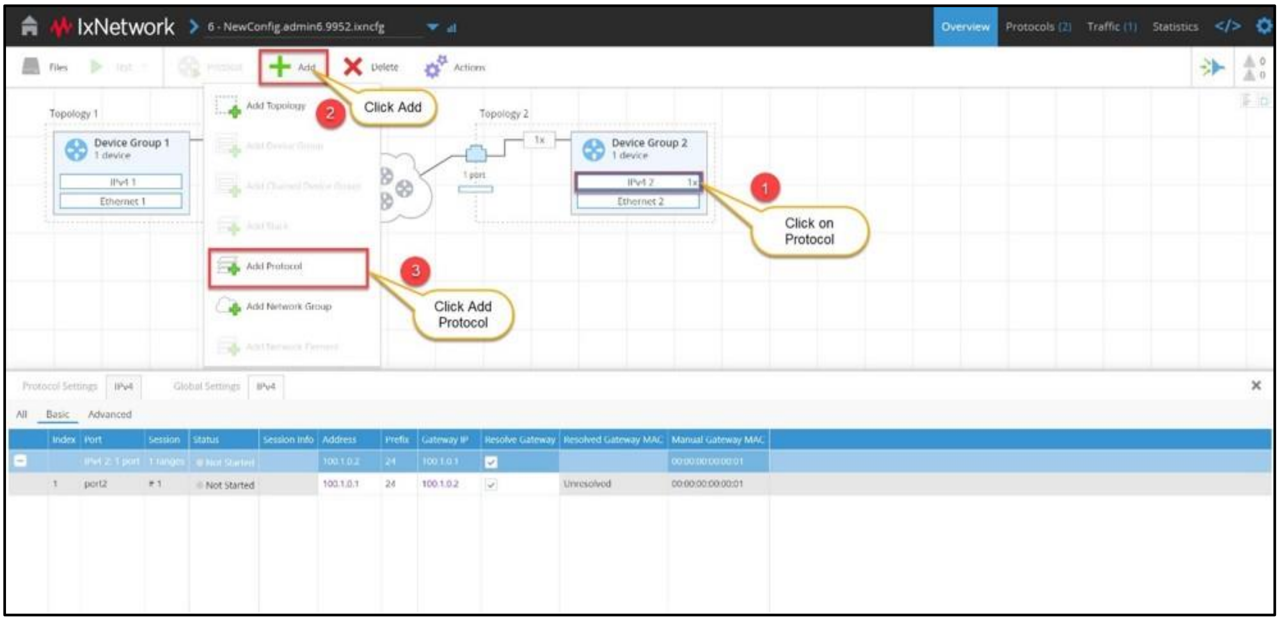
4 Click IPv4

5 Click IPv4

Fig 3.3 Add Chassis and Assign ports

3.4. Add OSPF on IPv4 Protocol

- User can add additional topologies, device groups and protocols by clicking **Add** tab.
- **Select Protocols** window allows user to choose the protocols as shown in Fig 3.4.2.
- Select OSPF protocol from **ROUTING/SWITCHING** section of **Select Protocols** window.

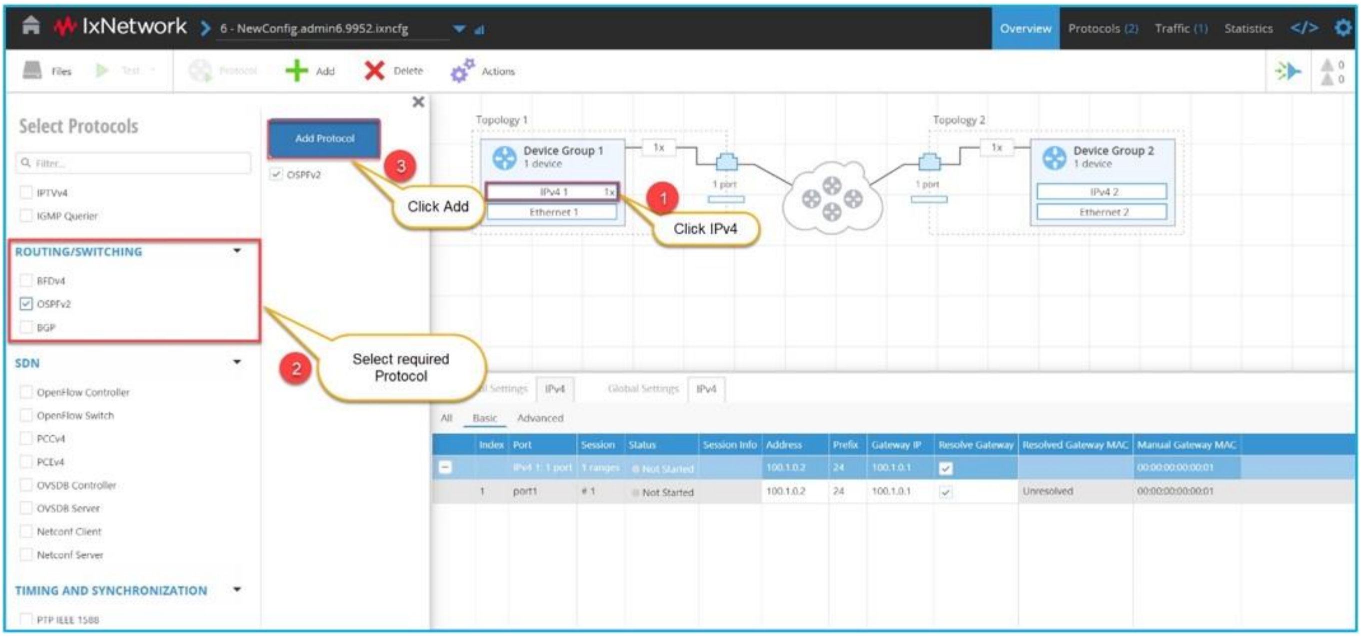


Protocol Settings | IPv4 | Global Settings | IPv4

All | Basic | Advanced

	Index	Port	Session	Status	Session Info	Address	Prefix	Gateway IP	Resolve Gateway	Resolved Gateway MAC	Manual Gateway MAC
−		IPv4 2: 1 port	1 ranges	Not Started		100.1.0.2	24	100.1.0.1	☑		00:00:00:00:00:01
	1	port2	# 1	Not Started		100.1.0.1	24	100.1.0.2	☑	Unresolved	00:00:00:00:00:01

Fig 3.4.1 Add OSPF on IPv4 Protocol



Select Protocols

Filter...

□ IPTVv4
□ IGMP Querier

ROUTING/SWITCHING
□ BFDv4
☑ OSPFv2
□ BGP

SDN
□ OpenFlow Controller
□ OpenFlow Switch
□ PCCv4
□ PCEv4
□ OVSDB Controller
□ OVSDB Server
□ Netconf Client
□ Netconf Server

TIMING AND SYNCHRONIZATION
□ PTP IEEE 1588

☑ OSPFv2

Settings | IPv4 | Global Settings | IPv4

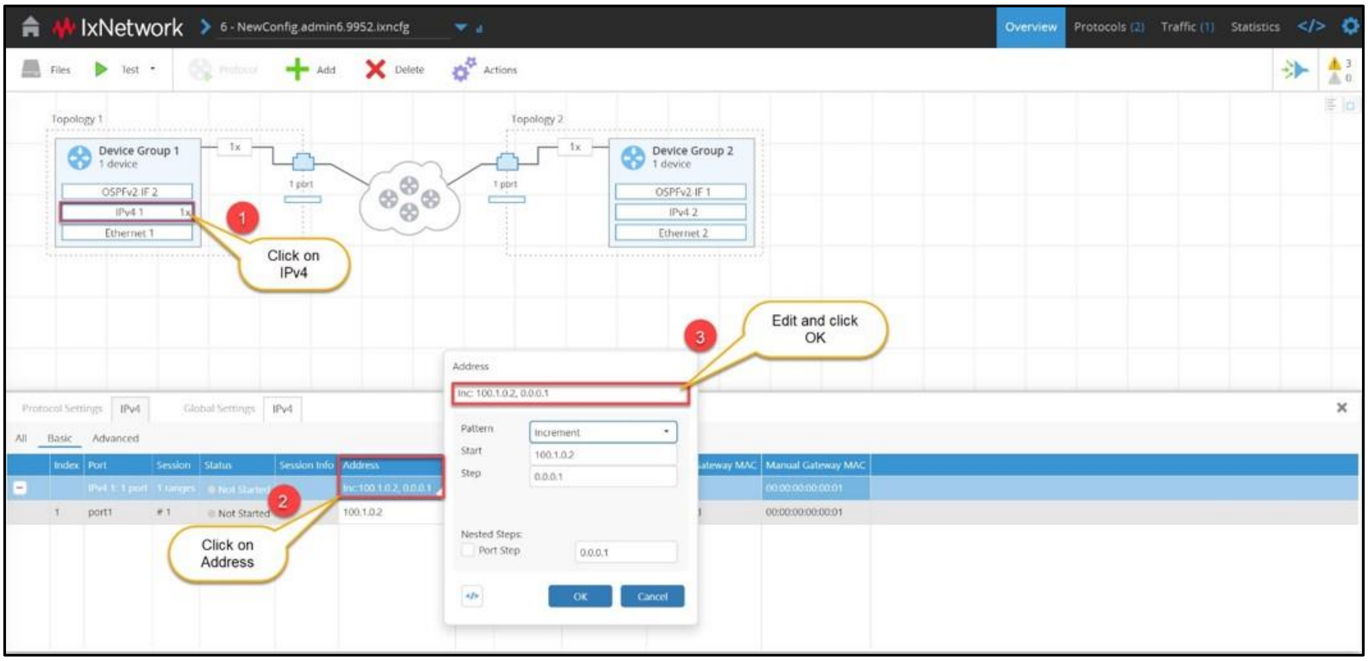
All | Basic | Advanced

	Index	Port	Session	Status	Session Info	Address	Prefix	Gateway IP	Resolve Gateway	Resolved Gateway MAC	Manual Gateway MAC
−		IPv4 1: 1 port	1 ranges	Not Started		100.1.0.2	24	100.1.0.1	☑		00:00:00:00:00:01
	1	port1	# 1	Not Started		100.1.0.2	24	100.1.0.1	☑	Unresolved	00:00:00:00:00:01

Fig 3.4.2 Select OSPF to add on IPv4

3.5. Edit protocol grid

- The interactive protocol grid appears at the bottom of the overview pagewhen particular protocol is selected.
- Edit the required fields and save the configuration.
- For example change the address and gateway for IPv4 protocol as shown below.



1 Click on IPv4

2 Click on Address

3 Edit and click OK

Address: Inc: 100.1.0.2, 0.0.0.1

Start: 100.1.0.2

Step: 0.0.0.1

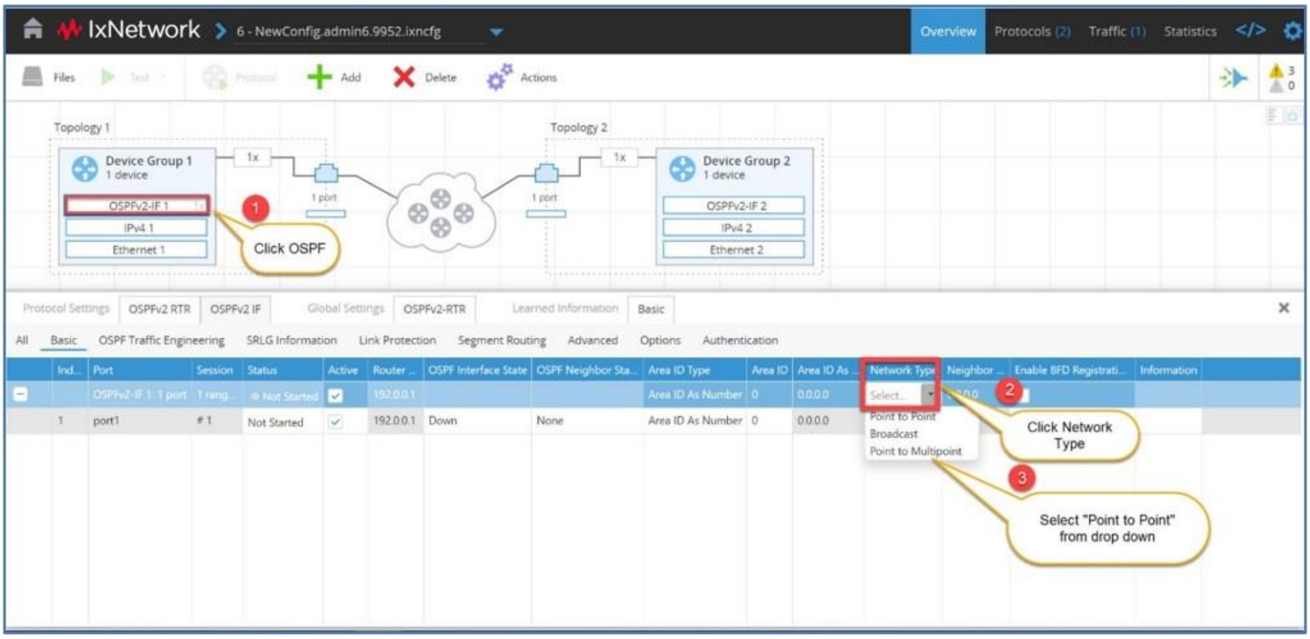
Port Step: 0.0.0.1

Index	Port	Session	Status	Session Info	Address	Manual Gateway MAC
	IPv4 1: 1 port	1 ranges	Not Started		Inc:100.1.0.2, 0.0.0.1	00:00:00:00:00:01
1	port1	#1	Not Started		100.1.0.2	00:00:00:00:00:01

Fig 3.5 Edit Protocol grid

3.6. Configure OSPF

- Edit OSPF protocol grid.
- Change the Network Type to Broadcast/Point to Point.



1 Click OSPF

2 Click Network Type

3 Select "Point to Point" from drop down

Ind...	Port	Session	Status	Active	Router ...	OSPF Interface State	OSPF Neighbor Sta...	Area ID Type	Area ID	Area ID As ...	Network Type	Neighbor ...	Enable BFD Registrati...	Information
	OSPFv2-IF 1: 1 port	1 rang...	Not Started	☑	192.0.0.1			Area ID As Number	0	0.0.0.0	Select...	0.0.0		
1	port1	#1	Not Started	☑	192.0.0.1	Down	None	Area ID As Number	0	0.0.0.0				

Fig 3.6 Configure OSPF

3.7. Run Test/Protocol

- User is provided with two options to run the protocols.
  - **Test** is a new utility which initiates complete test scenario in one shot. It includes connecting to ports and starting protocols followed by starting Traffic.
  - Start **Protocol,** starts all protocols configured in the test session.

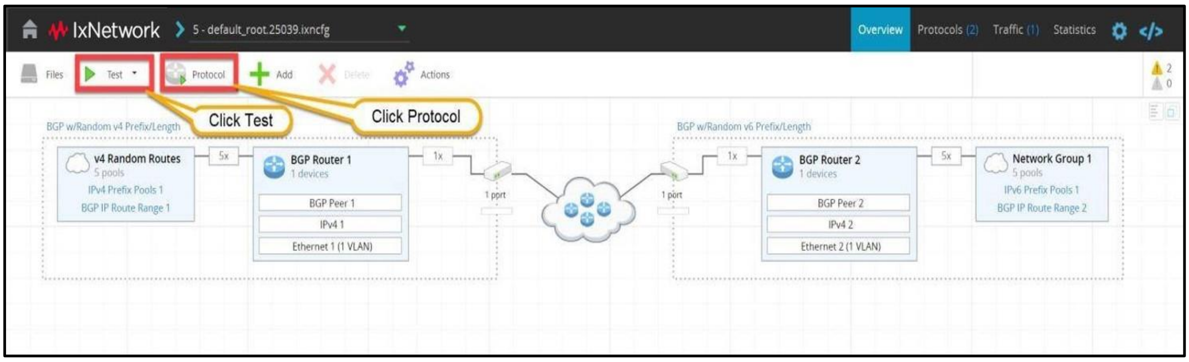
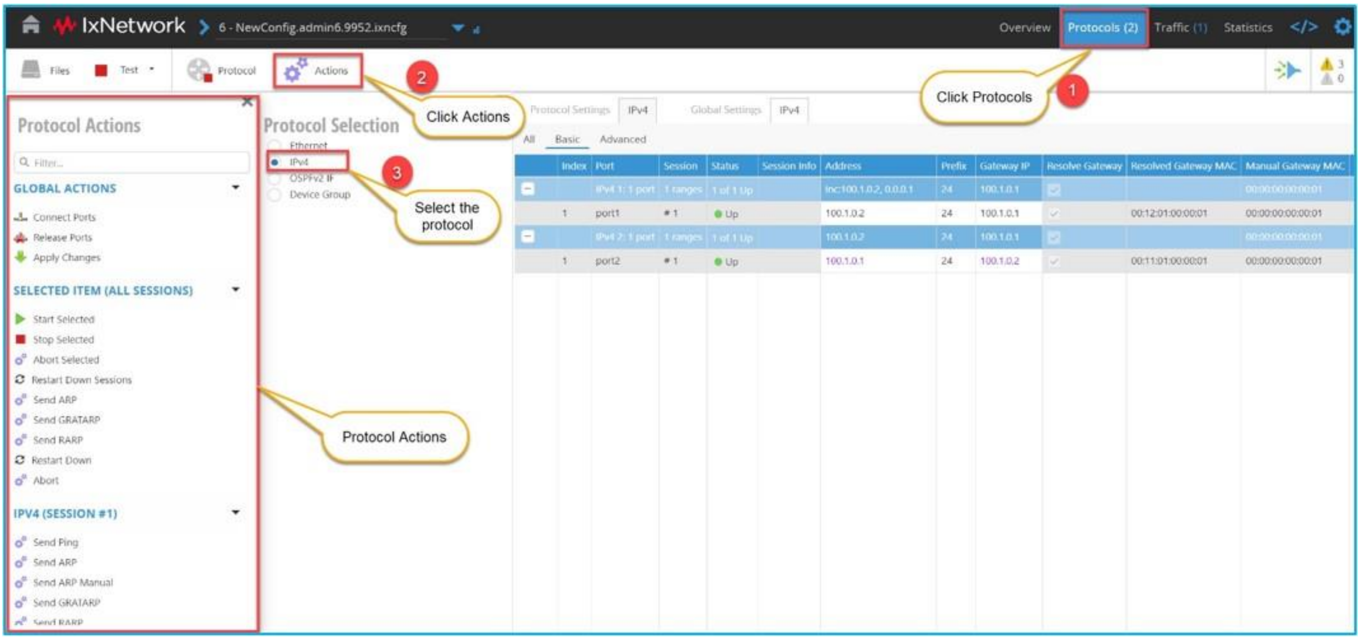


Fig 3.7 Run Test/Protocol

3.8. Protocol Actions

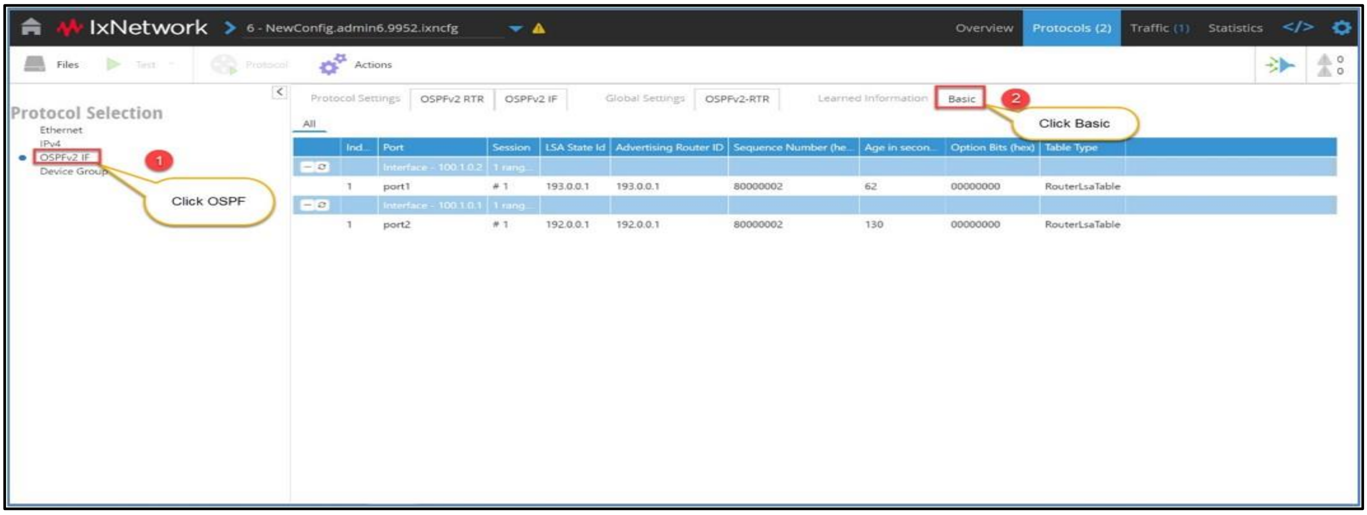
- Web App has provision to view details of all the protocols in **Protocols** page.
- User can choose the required protocol and the category from the drop down.
- Different protocol actions can be performed by selecting from the list of actions.



	Index	Port	Session	Status	Session Info	Address	Prefix	Gateway IP	Resolve Gateway	Resolved Gateway MAC	Manual Gateway MAC
−		IPv4 1: 1 port	1 ranges	1 of 1 Up		Inc:100.1.0.2, 0.0.0.1	24	100.1.0.1	☑		00:00:00:00:00:01
	1	port1	# 1	● Up		100.1.0.2	24	100.1.0.1	✓	00:12:01:00:00:01	00:00:00:00:00:01
−		IPv4 2: 1 port	1 ranges	1 of 1 Up		100.1.0.2	24	100.1.0.1	☑		00:00:00:00:00:01
	1	port2	# 1	● Up		100.1.0.1	24	100.1.0.2	✓	00:11:01:00:00:01	00:00:00:00:00:01

Fig 3.8 Protocol Actions

- Select "Learned info Basic" from protocol options to see the OSPF learned information



	Ind...	Port	Session	LSA State Id	Advertising Router ID	Sequence Number (he...	Age in secon...	Option Bits (hex)	Table Type
− ⟳		Interface - 100.1.0.2	1 rang...						
	1	port1	# 1	193.0.0.1	193.0.0.1	80000002	62	00000000	RouterLsaTable
− ⟳		Interface - 100.1.0.1	1 rang...						
	1	port2	# 1	192.0.0.1	192.0.0.1	80000002	130	00000000	RouterLsaTable

Fig 3.9 OSPF learned info

3.9. Add Traffic item

- Configures the traffic streams on the specified ports.
- Select Traffic type from the dropdown list Ex : IPv4.
- Choose Source and Destination from **Add Traffic** window.

*Changing Mesh settings is optional

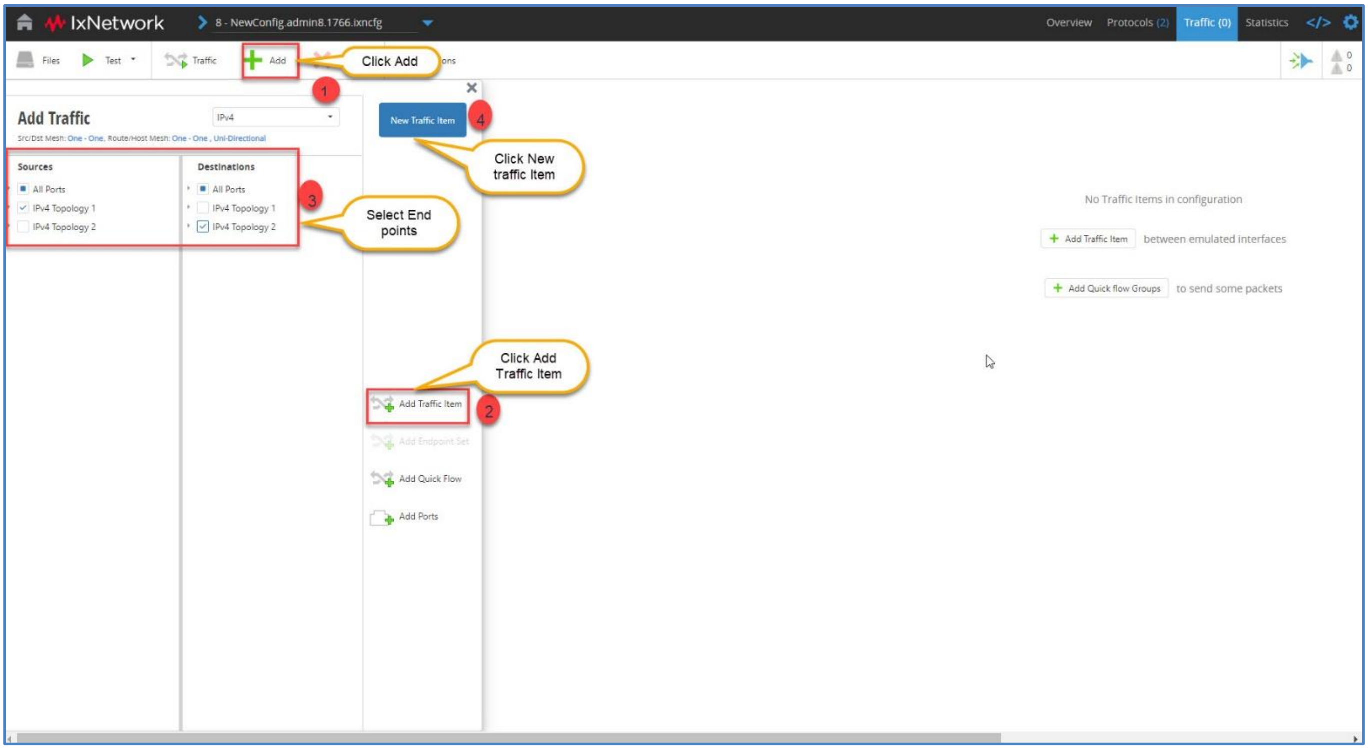
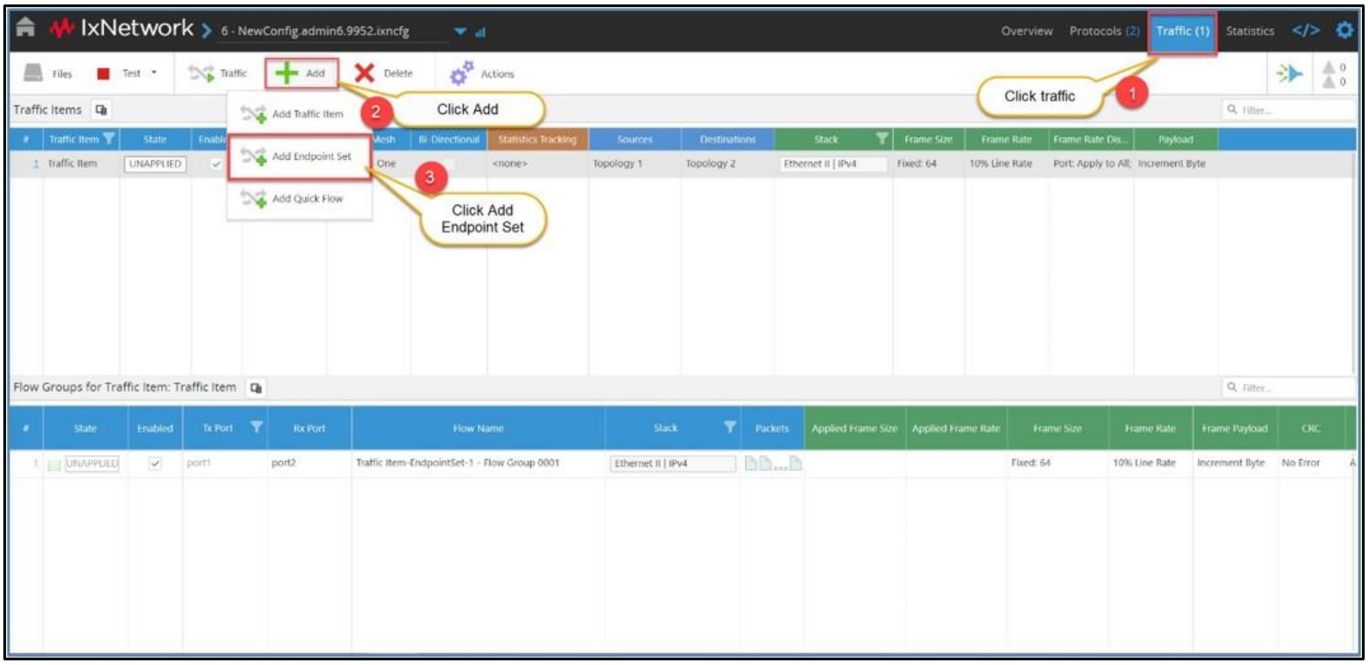


Fig 3.9 Add Traffic item

- Add ‘Endpoint Set’ by selecting source and destination by selecting respective topology



#	Traffic Item	State	Enabl	Mesh	Bi-Directional	Statistics Tracking	Sources	Destinations	Stack	Frame Size	Frame Rate	Frame Rate Dis...	Payload
1	Traffic Item	UNAPPLIED	✓	One		<none>	Topology 1	Topology 2	Ethernet II | IPv4	Fixed: 64	10% Line Rate	Port: Apply to All;	Increment Byte

Flow Groups for Traffic Item: Traffic Item

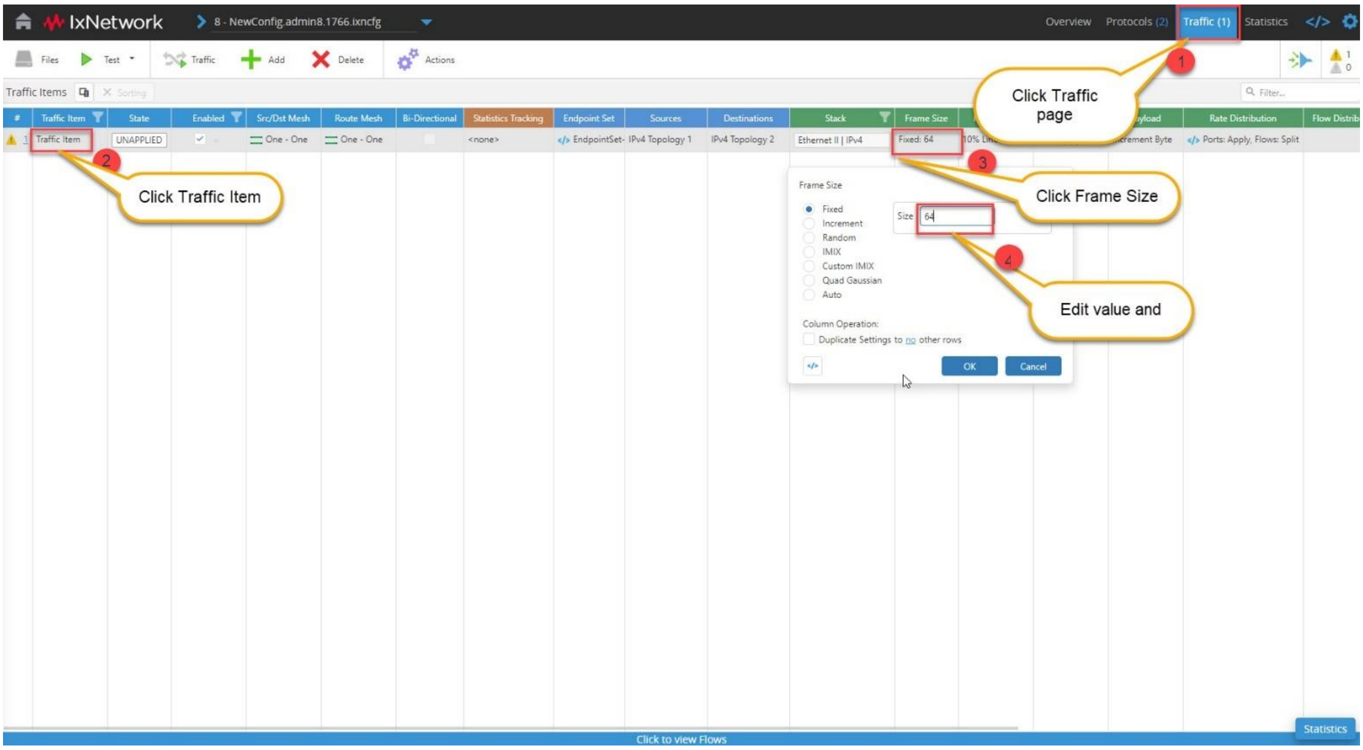
#	State	Enabled	Tx Port	Rx Port	Flow Name	Stack	Packets	Applied Frame Size	Applied Frame Rate	Frame Size	Frame Rate	Frame Payload	CRC
1	UNAPPLIED	✓	port1	port2	Traffic Item-EndpointSet-1 - Flow Group 0001	Ethernet II | IPv4				Fixed: 64	10% Line Rate	Increment Byte	No Error

Fig 3.10 Add Endpoint Set

3.10. Edit packet and setup flow groups

- ➢ Click on **Traffic item** to view flow groups grid.
- ➢ **Traffic Item** and **Flow Groups** grids are interactive, user can edit the fields and save the configuration.
- ➢ Create the flow groups based on the selectable packet fields, One flow group/high-level stream is created for each selected field.

*Editing the traffic item and setting up the flow group is optional



1 Click Traffic page

2 Click Traffic Item

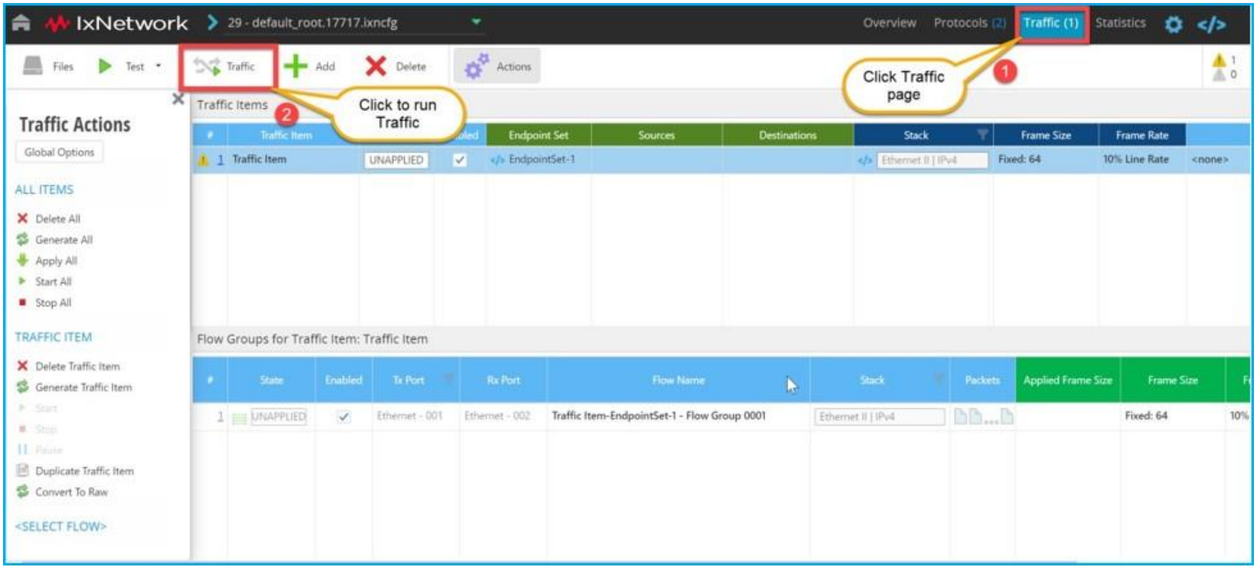
3 Click Frame Size

4 Edit value and

Fig 3.11 Edit Packet and setup flow groups

3.11. Start Traffic

- ➢ Start the traffic from **Traffic** page.



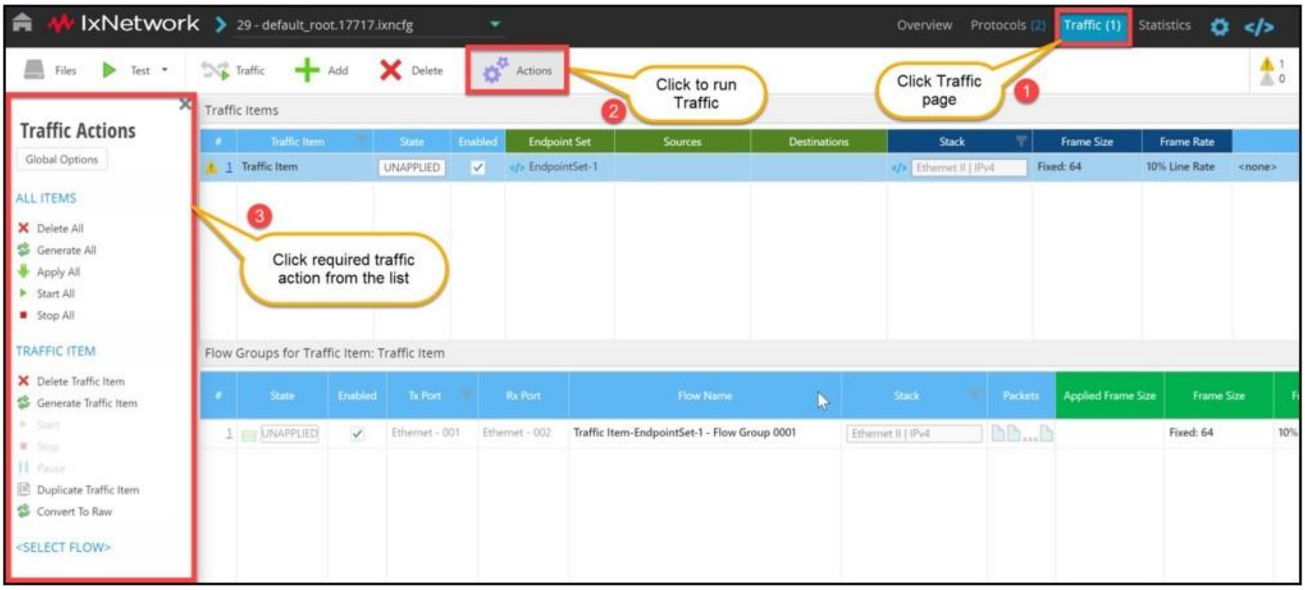
1 Click Traffic page

2 Click to run Traffic

Fig 3.12 Start Traffic

3.12. Traffic actions

- ➢ Similar to protocol actions, **Traffic Actions** allows user to perform different actions related to traffic.
- ➢ User can perform different traffic actions from the list shown in Fig 3.13



1 Click Traffic page

2 Click to run Traffic

3 Click required traffic action from the list

Traffic Items

#	Traffic Item	State	Enabled	Endpoint Set	Sources	Destinations	Stack	Frame Size	Frame Rate	
1	Traffic Item	UNAPPLIED	✓	EndpointSet-1			Ethernet II | IPv4	Fixed: 64	10% Line Rate	<none>

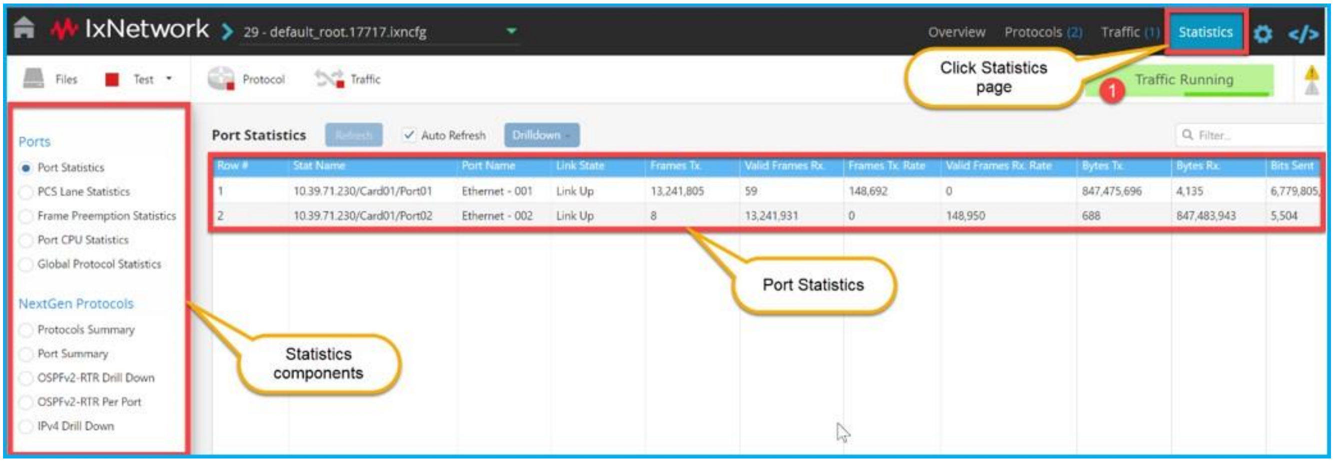
Flow Groups for Traffic Item: Traffic Item

#	State	Enabled	Tx Port	Rx Port	Flow Name	Stack	Packets	Applied Frame Size	Frame Size	F
1	UNAPPLIED	✓	Ethernet - 001	Ethernet - 002	Traffic Item-EndpointSet-1 - Flow Group 0001	Ethernet II | IPv4			Fixed: 64	10%

Fig 3.13 Traffic actions

3.13. View Statistics

- ➢ User can view traffic statistics from Statistics page.



1 Click Statistics page

Statistics components

Port Statistics

Port Statistics

Row #	Stat Name	Port Name	Link State	Frames Tx.	Valid Frames Rx.	Frames Tx. Rate	Valid Frames Rx. Rate	Bytes Tx.	Bytes Rx.	Bits Sent
1	10.39.71.230/Card01/Port01	Ethernet - 001	Link Up	13,241,805	59	148,692	0	847,475,696	4,135	6,779,805,
2	10.39.71.230/Card01/Port02	Ethernet - 002	Link Up	8	13,241,931	0	148,950	688	847,483,943	5,504

Fig 3.14 View Statistics

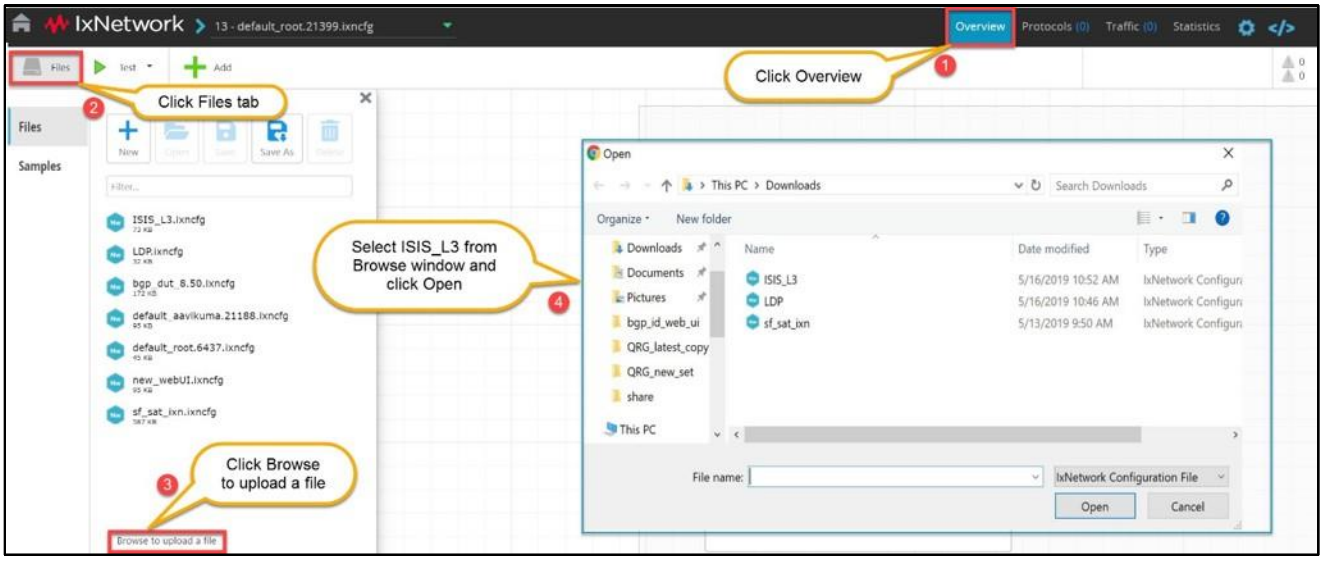
4. Configure a Test scenario using config file

This section walks through a scenario in which user is allowed to configure a test scenario by uploading ixncfg or json configuration files from **Files** tab, and user can also save the current configuration.

4.1. Upload the Config File

- ➢ Click **Browse to upload file** from **Files** tab to upload ixncfg config file, for example upload ISIS_L3.ixncfg.
- ➢ After uploading the ISIS_L3.ixncfg, follow the steps from section 2.4 to **2.10** to bring up

the test scenario.



1 Click Overview

2 Click Files tab

3 Click Browse to upload a file

4 Select ISIS_L3 from Browse window and click Open

Fig 4.1.1 Upload config file

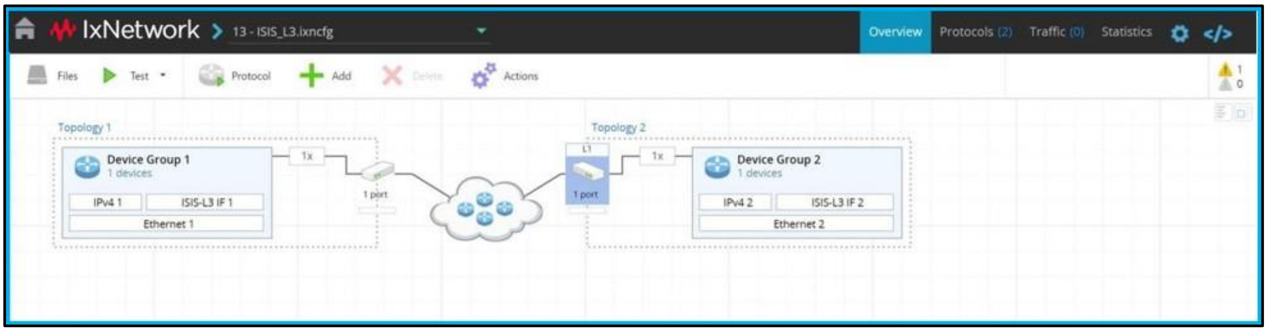
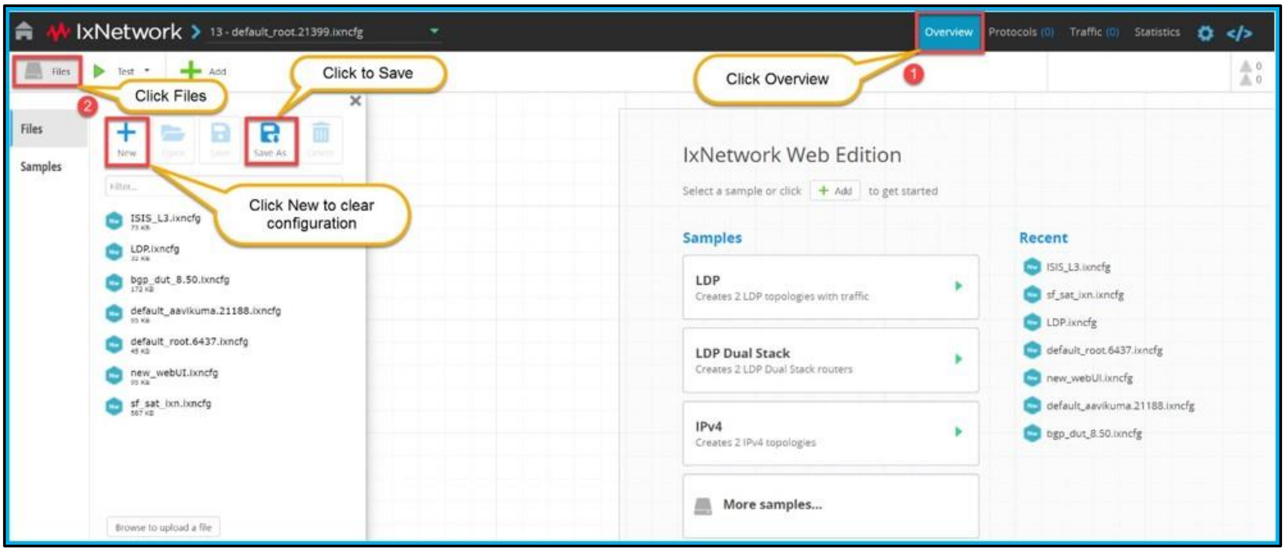


Fig 4.1.2 After uploading ISIS_L3.ixncfg

4.2. Save and Clear the configuration

- ➢ User can save and clear the current configuration from **Files** tab.



1 Click Overview

2 Click Files

Click to Save

Click New to clear configuration

Fig 4.2 Save and Clear Configuration

5. Other Utilities

This section covers additional capabilities of Web App.

5.1. IxNetwork API Browser

- The main feature of this application is the ability to browse the API data in a hierarchical format. Access each level of the hierarchy with a view of siblings, attributes, execs, errors, and children.

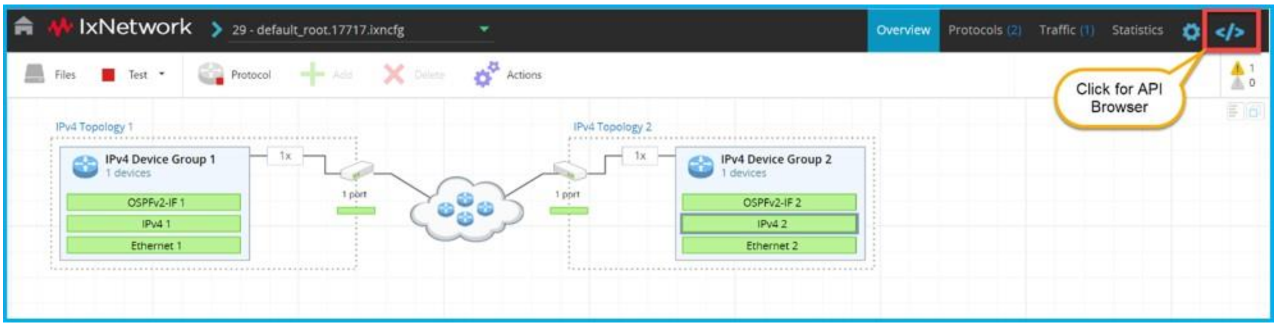
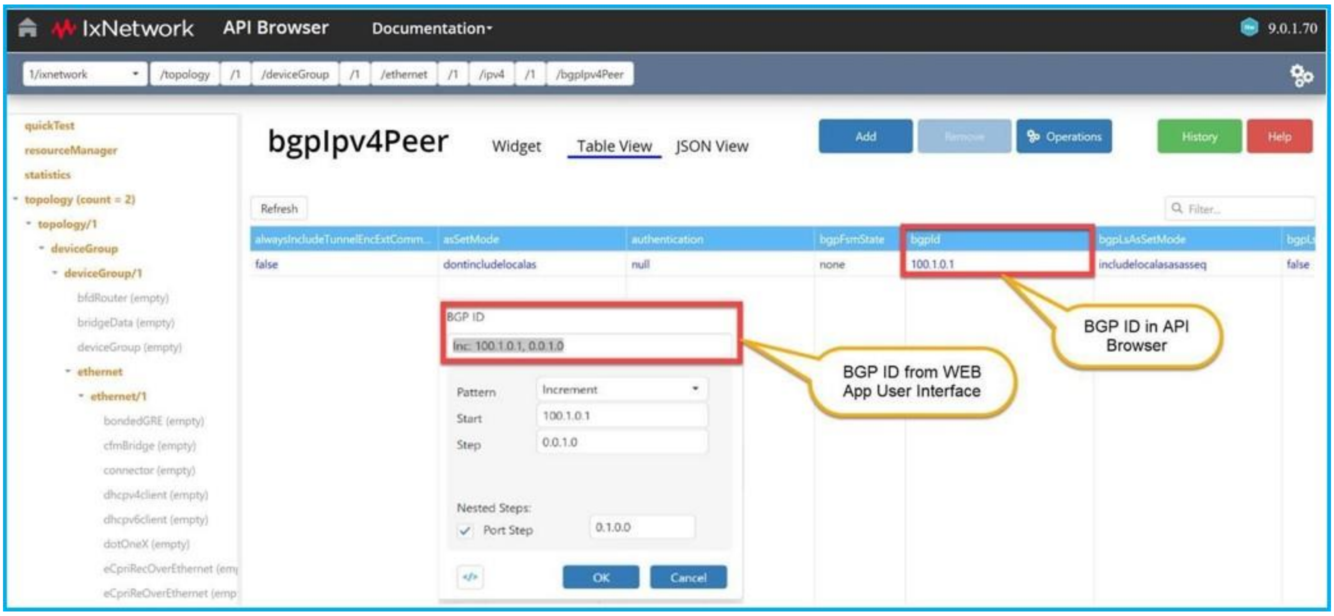


Fig 5.1.1 IxNetwork API documentation link



alwaysIncludeTunnelEncExtComm...	asSetMode	authentication	bgpFsmState	bgpId	bgpLsAsSetMode	bgpL
false	dontincludelocalas	null	none	100.1.0.1	includelocalasasasseq	false

BGP ID
Inc: 100.1.0.1, 0.0.1.0

Pattern: Increment
Start: 100.1.0.1
Step: 0.0.1.0

Nested Steps:
☑ Port Step: 0.1.0.0

Fig 5.1.2 IxNetwork API Browser

6. References

Linux API Server: https://www.youtube.com/watch?v=qSkgQvhGUeY&t=1s

Ixia Training Tv: https://www.youtube.com/channel/UCanJDvvWxCFPWmHUOOlUPIQo

Black books:
https://www.ixiacom.com/resources?field_resource_topic_target_id=271&field_resource_type_target_id=180&field_industries_target_id=All&combine=&items_per_page=28

7. Support

For more information, please visit the Ixia site (https://support.ixiacom.com/)

For support assistance, please contact (Support-India@ixiacom.com)