Black Book

Edition 10

Network Convergence Testing

Your feedback is welcome

Our goal in the preparation of this Black Book was to create high-value, high-quality content. Your feedback is an important ingredient that will help guide our future books.

If you have any comments regarding how we could improve the quality of this book, or suggestions for topics to be included in future Black Books, please contact us at ProductMgmtBooklets@ixiacom.com.

Your feedback is greatly appreciated!

Contents

How to Read this Book

The book is structured as several standalone sections that discuss test methodologies by type. Every section starts by introducing the reader to relevant information from a technology and testing perspective.

Each test case has the following organization structure:

Overview	Provides background information specific to the test case.
Objective	Describes the goal of the test.
Setup	An illustration of the test configuration highlighting the test ports, simulated elements and other details.
Step-by-Step Instructions	Detailed configuration procedures using Ixia test equipment and applications.
Test Variables	A summary of the key test parameters that affect the test's performance and scale. These can be modified to construct other tests.
Results Analysis	Provides the background useful for test result analysis, explaining the metrics and providing examples of expected results.
Troubleshooting and Diagnostics	Provides guidance on how to troubleshoot common issues.
Conclusions	Summarizes the result of the test.

Typographic Conventions

In this document, the following conventions are used to indicate items that are selected or typed by you:

- **Bold** items are those that you select or click on. It is also used to indicate text found on the current GUI screen.
- *Italicized* items are those that you type.

Dear Reader

Ixia's Black Books include a number of IP and wireless test methodologies that will help you become familiar with new technologies and the key testing issues associated with them.

The Black Books can be considered primers on technology and testing. They include test methodologies that can be used to verify device and system functionality and performance. The methodologies are universally applicable to any test equipment. Step by step instructions using Ixia's test platform and applications are used to demonstrate the test methodology.

This tenth edition of the black books includes twenty two volumes covering some key technologies and test methodologies:

Volume 1 – Higher Speed Ethernet

Volume 2 – QoS Validation

Volume 3 – Advanced MPLS

Volume 4 – LTE Evolved Packet Core

Volume 5 – Application Delivery

Volume 6 – Voice over IP

Volume 7 – Converged Data Center

Volume 8 – Test Automation

Volume 9 – Converged Network Adapters

Volume 10 – Carrier Ethernet

Volume 11 – Ethernet Synchronization

Volume 12 – IPv6 Transition Technologies

Volume 13 – Video over IP

Volume 14 – Network Security

Volume 15 – MPLS-TP

Volume 16 – Ultra Low Latency (ULL) Testing

Volume 17 – Impairments

Volume 18 – LTE Access

Volume 19 – 802.11ac Wi-Fi Benchmarking

Volume 20 – SDN/OpenFlow

Volume 21 – Network Convergence Testing

Volume 22 – Testing Contact Centers

A soft copy of each of the chapters of the books and the associated test configurations are available on Ixia's Black Book website at http://www.ixiacom.com/blackbook. Registration is required to access this section of the Web site.

At Ixia, we know that the networking industry is constantly moving; we aim to be your technology partner through these ebbs and flows. We hope this Black Book series provides valuable insight into the evolution of our industry as it applies to test and measurement. Keep testing hard.

Errol Ginsberg, Acting CEO

Network Convergence Testing

Test Methodologies

The Network Convergence Testing booklet provides various measuring techniques designed to characterize how quickly the DUT recovers from route convergence or fail-over. It covers the relevant industry standards and explains how to apply them to obtain consistent benchmark test results.

Convergence Testing

Failover is the capability to automatically switch over to a redundant or standby network path during a failure or abnormal termination of a network. Failover happens without human intervention and generally without warning. Failback is the process of restoring a network in the failover state back to its original state (before failure).

Convergence occurs when a failure or abnormal event causes the network to move traffic from a primary path to a backup path. Route convergence is complete when all of the route addresses are updated and traffic to the affected routes has switched from the primary to secondary (failover) path. This is due to the fact that IP networks use addressing for each segment of the network.

Network components such as routers and switches typically implement failover capability through protocols or protocol extensions. Networks carry critical data and require continuous availability and a high degree of reliability.

Layer 3 routing protocols such as RIP, OSPF, ISIS, and BGP provide the capability to re-route IP traffic if a network or link goes down. In the event of a link failure, layer 2 protocols such as STP/RSTP/MSTP and LDP/RSVP-TE provide traffic re-direction mechanisms. Due to increased and more complex traffic demands, next generation network (NGN) convergence times must be faster than current convergence times. Strategies and protocols to implement convergence in NGNs include:

- Graceful restart
- Hitless restart
- Virtual router redundancy protocol
- MPLS fast re-route
- Bi-directional forwarding detection,
- Link OAM/CFM
- Protocol timer manipulation

Service providers guarantee customers a specific level of service and close to 99.999% network uptime through service level agreements (SLAs). Challenging SLA requirements mandate that service providers enable features that minimize downtime and enact rapid convergence. Mission-critical applications such as financial and emergency services cannot accept downtime and require high-availability networks.

Metrics for Network Uptime

Uptime (%)	Downtime
90%	876 hours (36.5 days)
95%	438 hours (18.25 days)
99%	87.6 hours (3.65 days)
99.9%	8.76 hours
99.99%	52.56 minutes
99.999%	5.256 minutes
99.9999%	31.536 seconds

Total network downtime is only about 5 minutes a year if **99.999%** of uptime is achieved.

Relevant Standards

- Benchmarking Methodology for Link-State IGP Data Plane Route Convergence as per RFC 6413
- Basic BGP Convergence Benchmarking Methodology for Data Plane Convergence as per draft-ietf-bmwg-bgp-basic-convergence

Measurements

Ixia's flagship IxNetwork application powered by ViperCore technology – introduces TrueView™ Convergence, the most comprehensive convergence test capability in the industry. Providing comprehensive measurements of network convergence requires the ability to:

- Timestamp every packet
- Timestamp the first packet in and last packet out on a port, per-flow
- Capture protocol event timestamps
- Capture link event timestamps
- Monitor Rx rate and timestamp when set below thresholds are crossed

- Monitor Rx Rate and timestamp when set above thresholds are crossed. Time-stamping the packet types listed above allows IxNetwork to monitor two critical measurements:
- Route convergence time -- from a triggering control plane event (such as BGP routes withdraw) to the resulting data plane switch from the primary to secondary path.
- Service interruption time – the time delta from the throughput dropped below and restored above user-defined threshold on the same RX path.

The following measurements are made in an IxNetwork convergence test, on a per-test basis:

- DP-Above-Threshold Timestamp
    - The hardware timestamp when a flow exceeds the user-defined throughput threshold; that is, Above Threshold Timestamp
    - Measured on secondary port for route convergence test, or on the same RX port for service interruption test
- DP-Below-Threshold timestamp
    - The hardware timestamp when a flow drops below the user-defined throughput threshold; that is, Below Threshold Timestamp
    - Measured on primary port for route convergence test, or on the same RX port for service interruption test
- Event (start/stop) timestamps
    - Value of the hardware timestamps when the control plane (For example, OSPF Route Flap) or link up/down event triggering Data Plane Switchover occurs starts/stops
    - The Event Start Timestamp is recorded when the first control plane update packet leaving Ixia TX port, or the simulated link down action is enabled at Ixia TX port.
    - The Event Stop Timestamp is recorded when the last control plane update packet leaving Ixia TX port.

Based on the recorded timestamps listed above, IxNetwork reports the following pre-defined convergence measurements:

- DP/DP convergence
    - Calculates the convergence time for the traffic flows to converge from a primary to secondary port
        - Secondary port DP-Above-Threshold timestamp – primary port DP-Below-Threshold timestamp
- CP/DP convergence
    - Calculates the convergence time from the start of the control plane event triggering data plane switchover to the traffic flows converging on the secondary port
        - Secondary port DP-Above-Threshold timestamp – Event Start timestamp
- Ramp-down time (primary port)
    - Calculates ramp-down time for the primary port from dropping the traffic flows until it stops receiving all traffic
        - Primary port last arrived packet timestamp – primary port DP-Below-Threshold timestamp

- Ramp-up time (secondary port)
  - Calculates the ramp-up time for the secondary port from receiving the first flow until it starts receiving all traffic
    - Secondary port DP-Above-Threshold timestamp – secondary port first arrived packet timestamp
- Service interruption time (SIT)
  - Calculate the time difference between DP-Above-Threshold timestamp and DP-Below-Threshold timestamp of the monitored traffic flows on the same RX path
    - SIT = DP-Above-Threshold timestamp – DP-Below-Threshold timestamp
    - SIT requires user to define it in **Flow Statistics** through client formula feature

Test Case: OSPF Routes Convergence Test

Overview

OSPF is one of the most important IGPs deployed in enterprise and carrier networks today. Its ability to recover from network failures is critical for operators to meet SLA.

Objective

The objective of this test is to measure the convergence time after an OSPF route flap causes the traffic of Device Under Test (DUT) to switch from the primary to a secondary path.

Setup

As depicted in the following figure, the test consists of a DUT and three Ixia test ports. Two Ixia test ports emulate two OSPF routers, which each advertise one route range per Ixia emulated router:

- Port 1 and Port 2 (OSPF R1, OSPF R2) advertise the same single route range. OSPF R1 advertises a lower metric for the advertised range.
- Since OSPF R1 advertises a lower destination metric, it is selected as the primary path. OSPF R2 is selected as the secondary path.

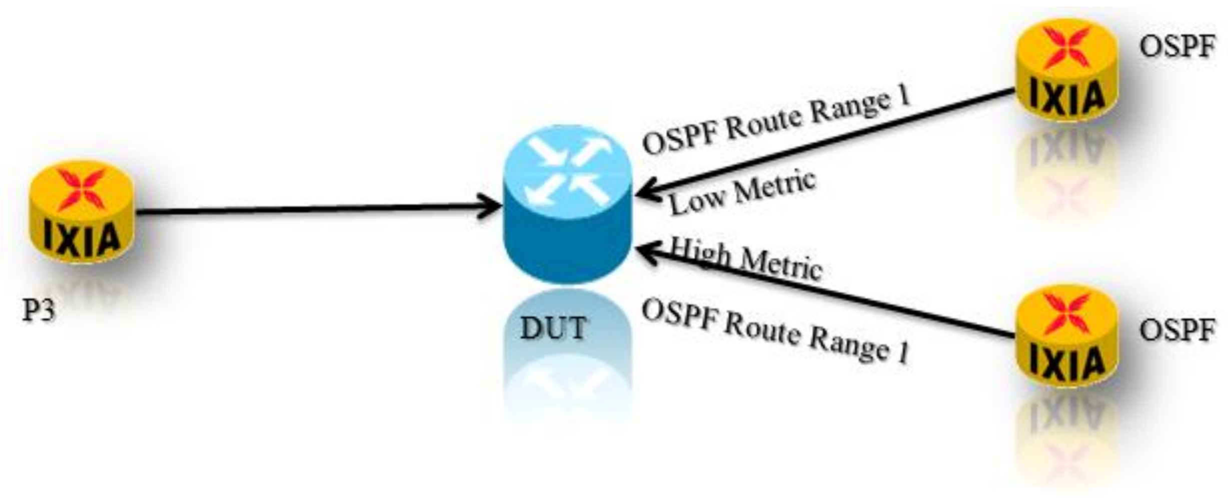


Figure 1. Ixia emulated OSPF topology

Step-by-Step Instructions

The following instructions assist in creating a convergence test as shown in the preceding figure. In addition, you can refer to these instructions as a guide for building many other convergence test scenarios.

1. Reserve three ports in IxNetwork.

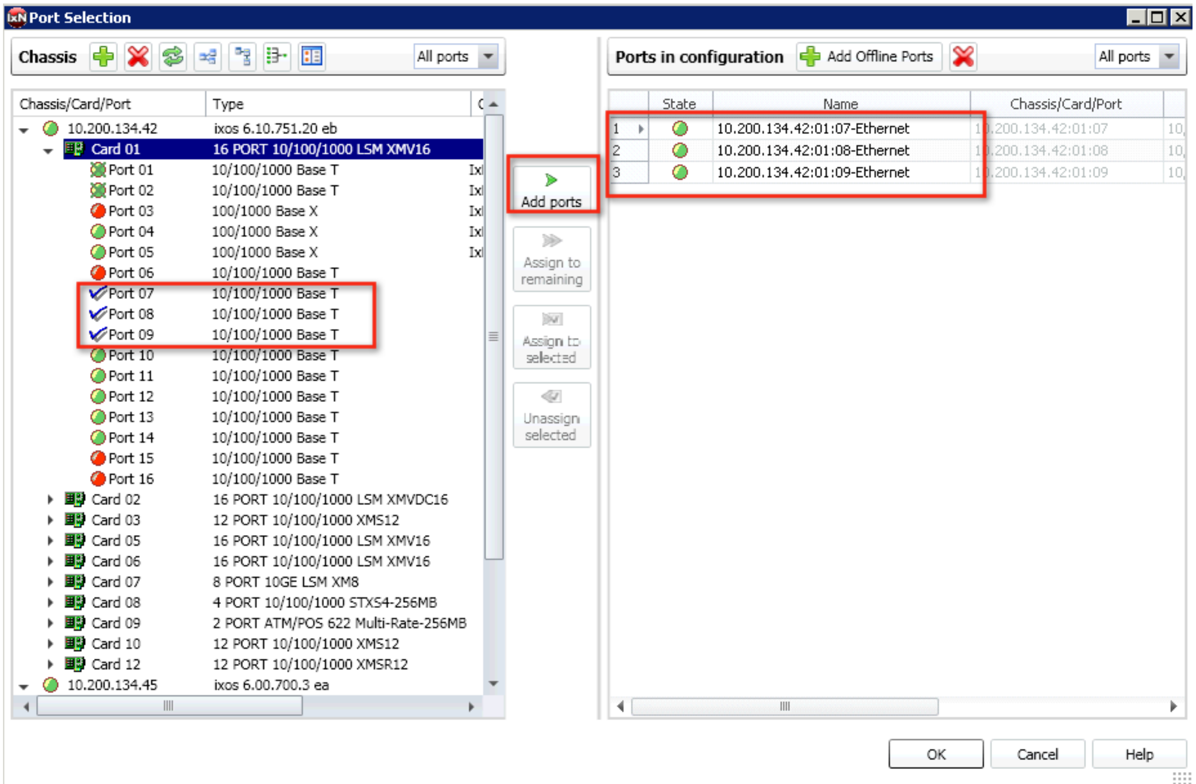


Figure 2. Port Reservation

2. Rename the ports for easier use throughout IxNetwork.

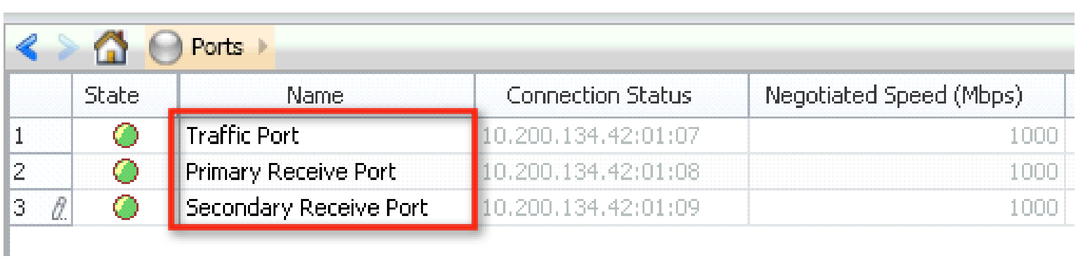


Figure 3. Port naming

3. In the IxNextwork application, click **Add Protocols**.

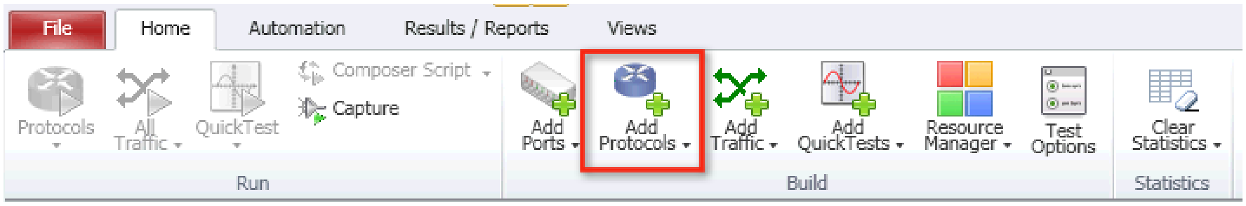


Figure 4. Protocol wizards

4. Run the **OSPF** protocol wizard.

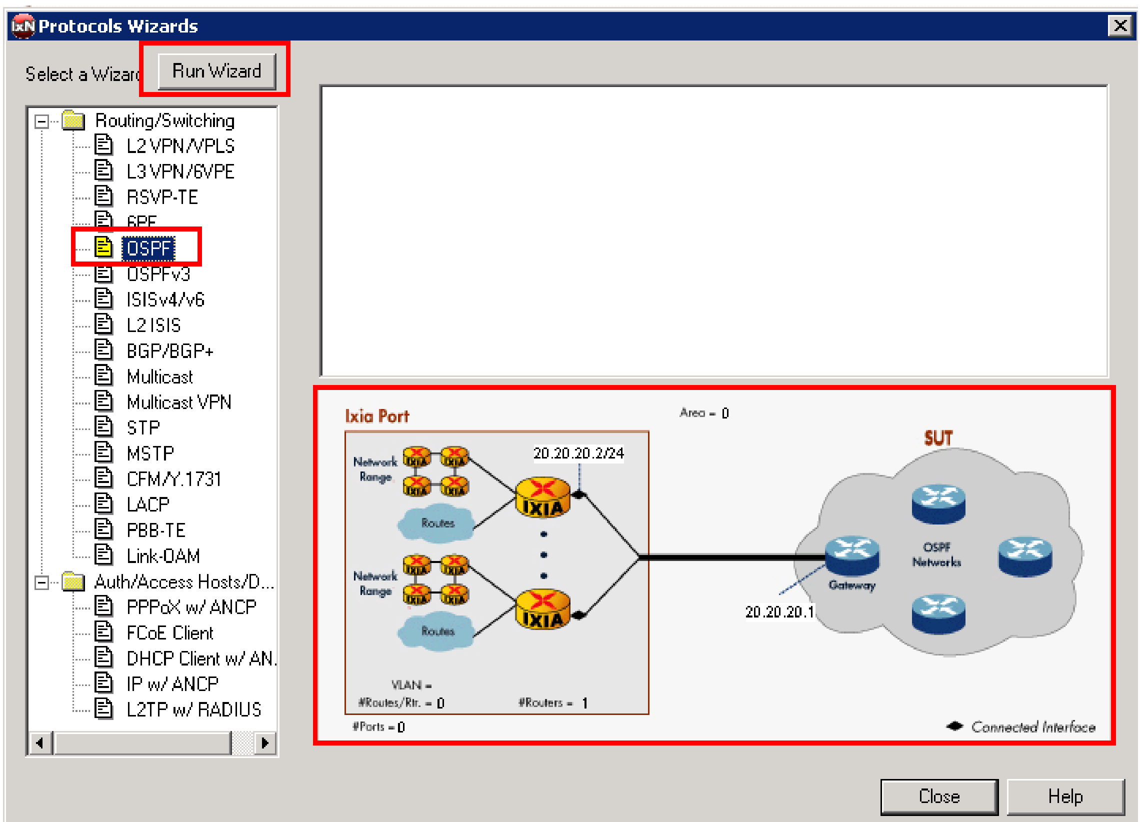


Figure 5. OSPF wizard

Note: The OSPF wizard graphic represents a typical test case for testing OSPF, regardless of whether it is a convergence test or not.

5. Configure **Primary Receive Port** and **Secondary Receive Port** (or whatever names were assigned) to emulate the OSPF Routers, and then click **Next**.

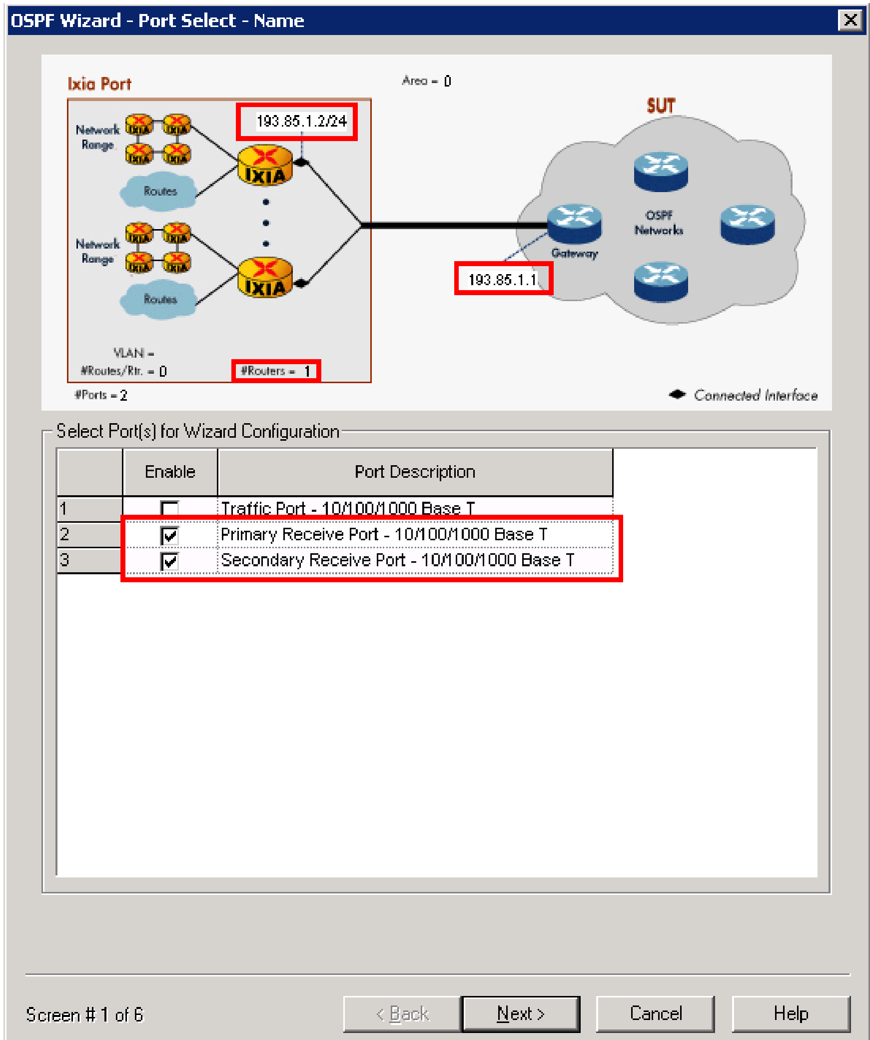


Figure 6. OSPF wizard screen 1 of 6

6. The **Routers** dialog configures the **Primary Receive Port** and **Secondary Receive Port** to emulate an OSPF router. These ports are configured to communicate directly with the DUT router.

    - Keep the default of *1* OSPF router. This is a per-port setting.
    - Keep the default of **OSPF Area ID (0.0.0.0)**
    - Configure the **Tester IP Address** and **Gateway** IP addresses
        i. In this test, they are *193.85.1.2/24* and *193.85.1.1/24* for the Primary Receive Port.
        ii. In this test, they are *194.85.1.2/24* and *194.85.1.1/24* for the Secondary Receive Port.
        iii. Set the **Increment Per Port** option to *1.0.0.0*, which configures the Secondary Receive Port IP address and gateway.
    - Click **Next**.

Optionally:

a. Select **Enable VLAN** if the DUT has VLANs enabled on the connected ports.
b. Change the **OSPF Area ID** to match the DUT settings for OSPF.

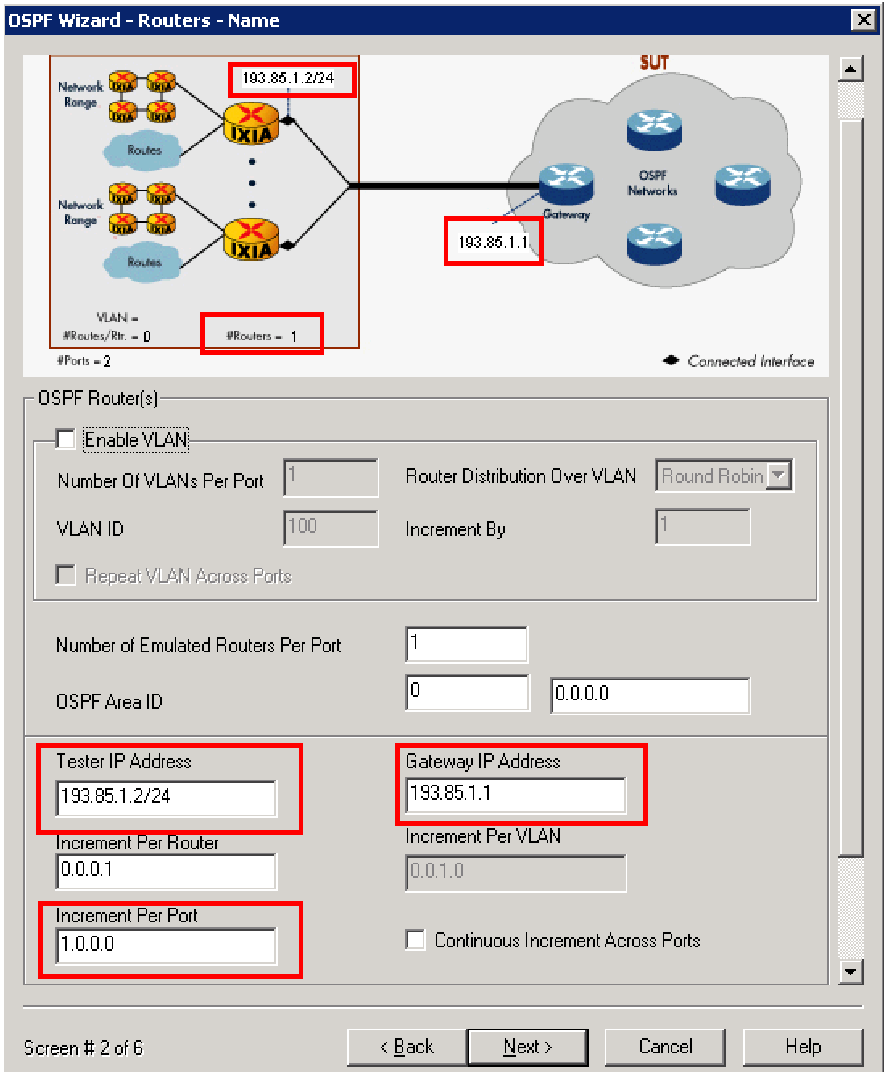


Figure 7. OSPF wizard screen 2 of 6

Note: The picture above updates with the configured IP addresses.

7. The **Route Ranges** dialog configures the route ranges to be advertised by the emulated OSPF Router on **Primary Receive Port** and **Secondary Receive Port.**

   a. Enable Advertise Routes

      Set the **Number of Routes per Router** to*1000* per router.

   b. Set the **First Route** of this route range to *131.1.1.0/24*.

      Set **Increment By (Per Router)** to *0.0.0.0*, because both OSPF routers must advertise the same routes.

   c. Keep the **Route Origin** to default.

   d. Keep the **Route Metric** to default.

   e. Click **Next**.

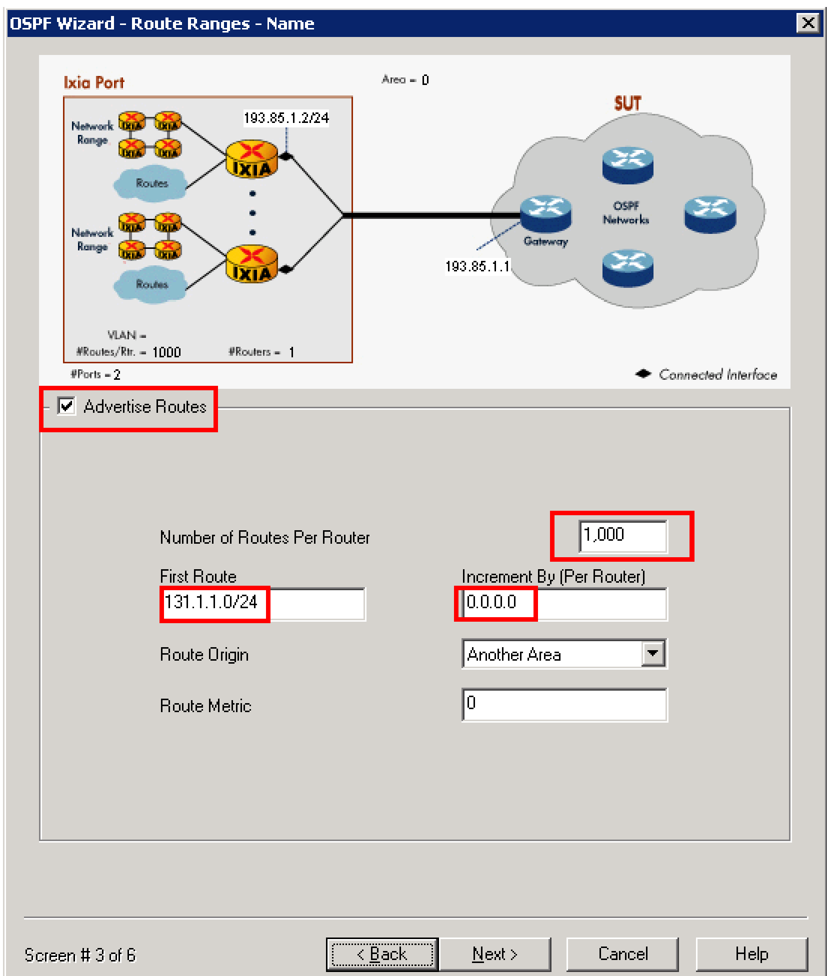


Figure 8. OSPF wizard screen 3 of 6

8. The **Network Range** dialog configures what network ranges are advertised by the emulated OSPF routers.

   a. Clear the **Advertise Network Range** check box.

   b. Click **Next**.

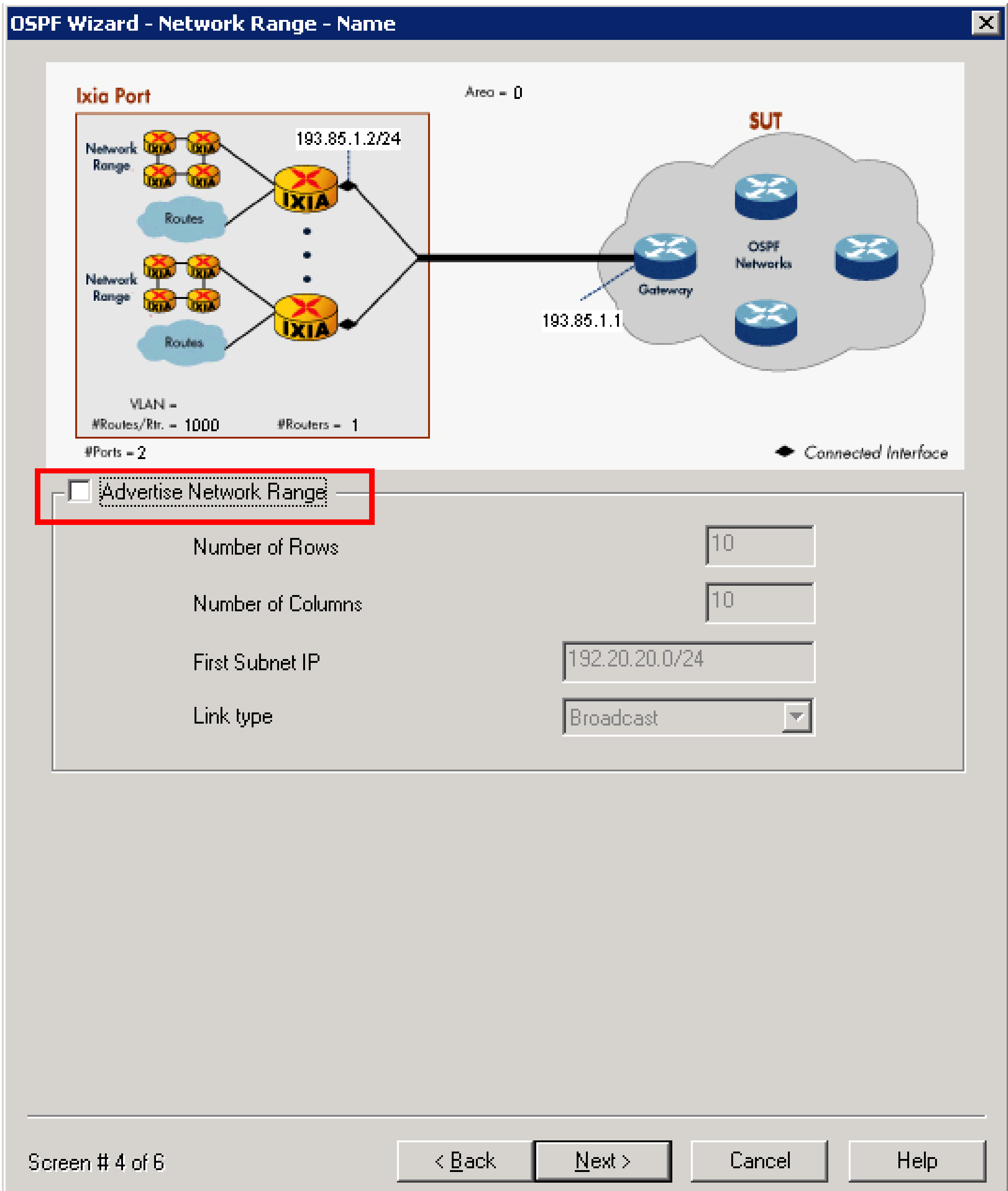


Figure 9. OSPF wizard screen 4 of 6

9. The **Interface TE** dialog configures the traffic engineering options advertised by the emulated OSPF Routers.

   a. Clear the **Enable Traffic Engineering for Connected Interface** check box.

   b. Click **Next.**

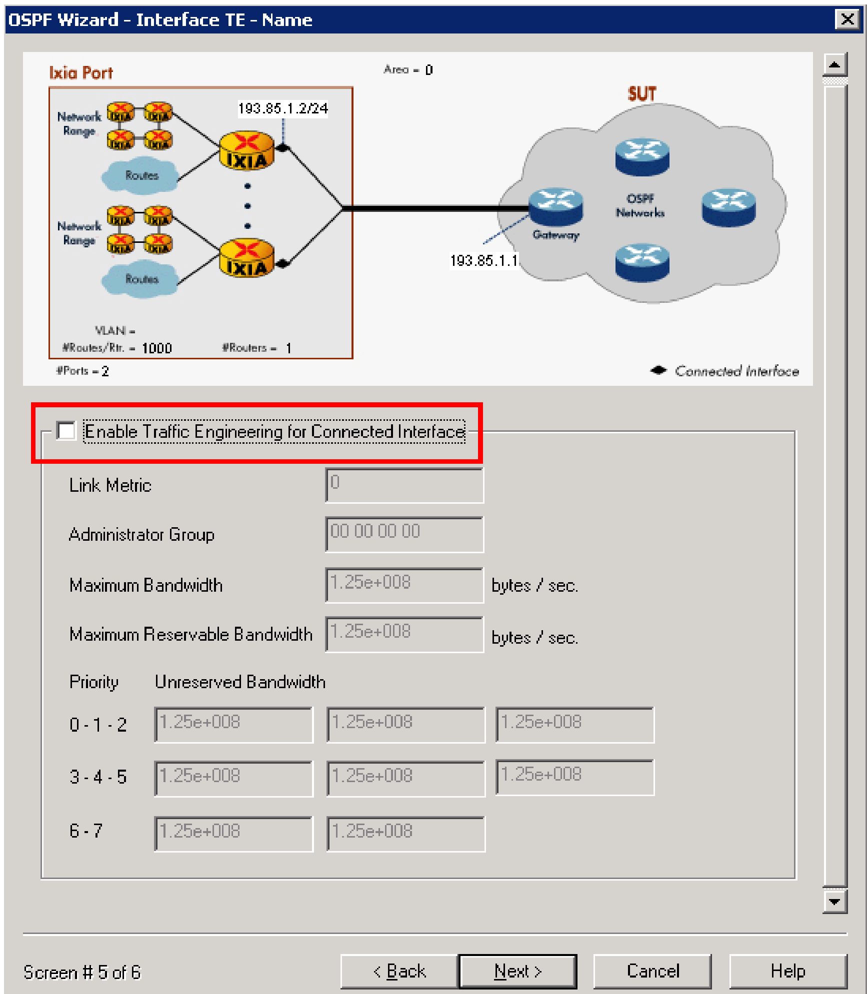


Figure 10. OSPF wizard screen 5 of 6

10. The **OSPF Primary and Secondary Port** dialog sets the test name and the action to take when the configured test is saved.

    a. Enter a description for the protocol configuration in the Name field. In this case use OSPF Primary and Secondary Port.

    b. Specify what to do with the finished test configuration.

    In this configuration, select **Generate and Overwrite Existing Configuration**. This task overwrites any previous protocol configuration.

    c. Click **Finish**.

Optionally:

a. Select **Save Wizard Config, But Do Not Generate on Ports**. This option saves the protocol configuration with the configured name, but does not modify the existing IxNetwork configuration.

b. Select **Generate and Overwrite Existing Configuration**. This option overwrites the protocol configuration, but appends IP addresses to the **Protocol Interfaces** configuration.

c. Select **Generate and Overwrite All Protocol Configurations**. This option removes all protocol and IP address configurations on the ports.

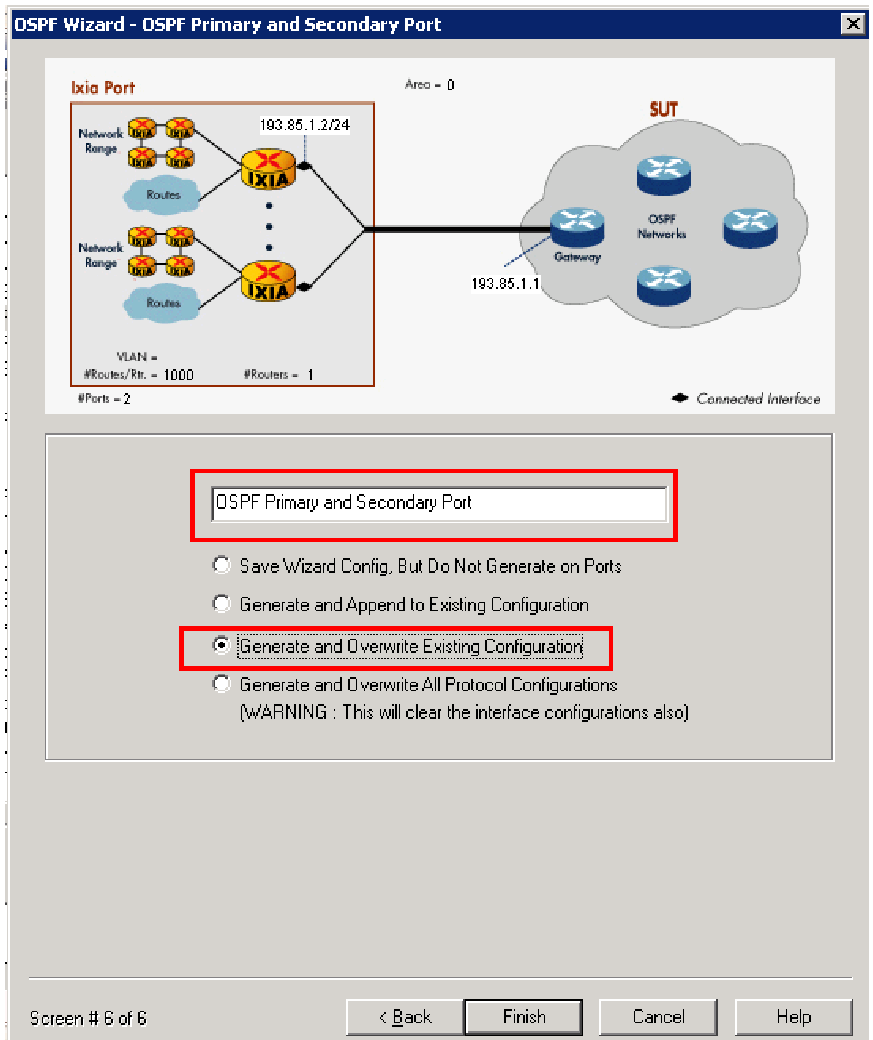


Figure 11. OSPF wizard screen 6 of 6

11. The **Protocol Wizard** dialog shows the saved protocol configuration template.

    a. Select **Close** to finish the protocol configuration

Optionally, with saved wizard templates you can:

a. Come back to the same protocol configuration to view and/or modify the configuration by double-clicking on the name.
b. Save new or modified protocol configurations with a different name, or overwrite existing templates.
c. Create a library of templates for use in different tests.
d. Highlight each template and preview the configuration in the topology, as shown in the following figure.

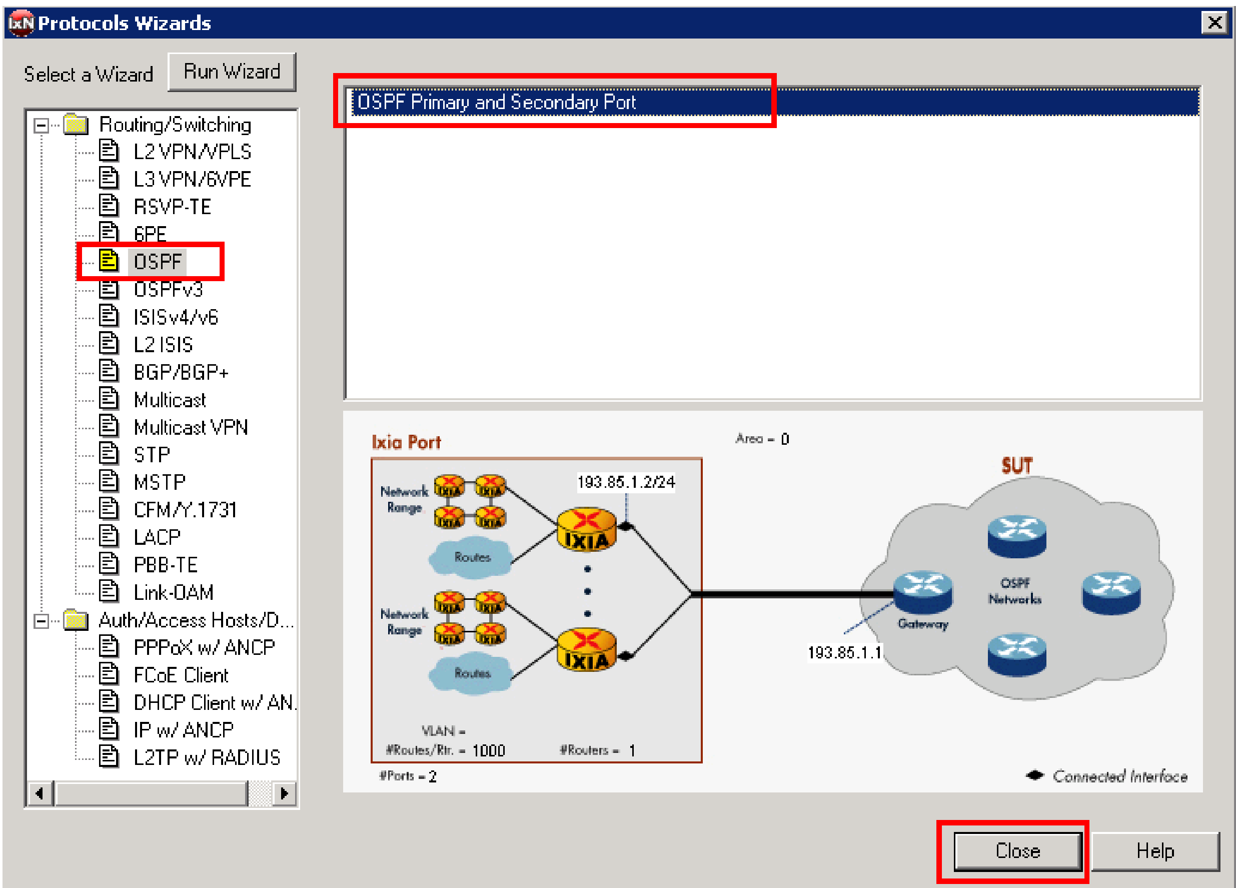


Figure 12. OSPF wizard saved wizard template

12. Once the wizard is complete, examine the contents of the IxNetwork configuration windows to see how the values were set. Verify IP connectivity between the DUT interfaces and the Ixia port interfaces. For example,

    a. Click the **Protocol Interfaces** in the **Test Configuration** panel.

        i. Verify that the IP addressing/incrementing functions of the wizard properly created IP interfaces that connect to the DUT, as shown in the following figure..

        ii. Add an IPv4 address to the **Traffic Port**. In this test, the **IPv4 Address** is *192.85.1.2/24* and the **Gateway** is *192.85.1.1/24.*

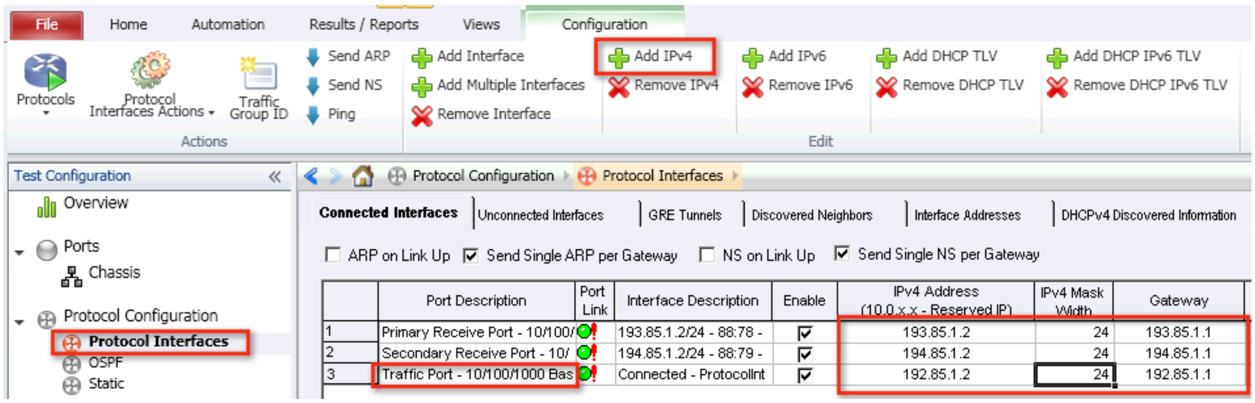


Figure 13. Protocol interface window

13. Check the protocol configuration. Make sure the settings work with the DUT's configuration. For example:
    a. Click **OSPF** in the **Test Configuration** panel.
    b. Note the two OSPF routers connected to the two DUT ports. If necessary, change any OSPF property to match the DUT settings.
    c. Set the **Metric** of the advertised routes:
        i. Change the routes advertised **Metric** of the primary receive port to *10.*
        ii. Change the routes advertised **Metric** of the secondary receive port to *20*.

Note. Advertising different metrics for the same routes creates a primary (preferred) and secondary (backup) path for traffic destined to the advertised routes.

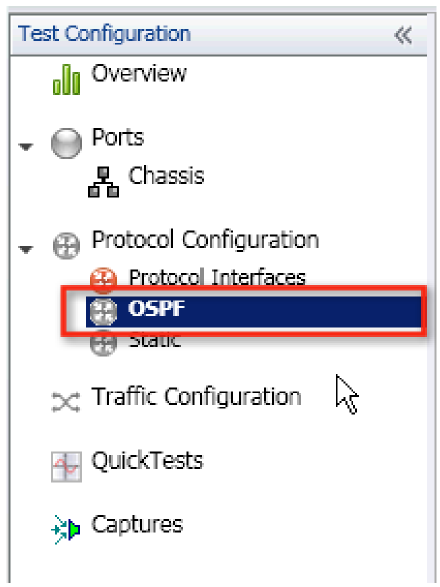


Figure 14. Selecting the OSPF Configuration

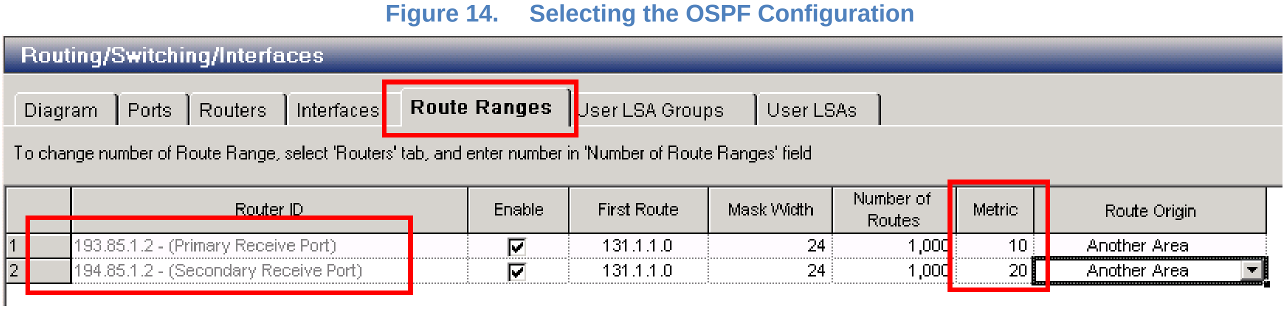


Figure 15. Protocol configuration window

14. . Click **Configuration** > **OSPF** > **Start All** as depicted in the figure below.

15. Check if all of the OSPF sessions are up.

    Troubleshooting:

    a. If the sessions are not up, go back to the **Test Configuration** window and double check the protocol configuration against the DUT.

    b. In the **Test Configuration** pane, click **Capture** and turn on **Control Plane Capture**, then start the **Capture** for a real-time sniffer analysis between the Ixia port and the DUT port.

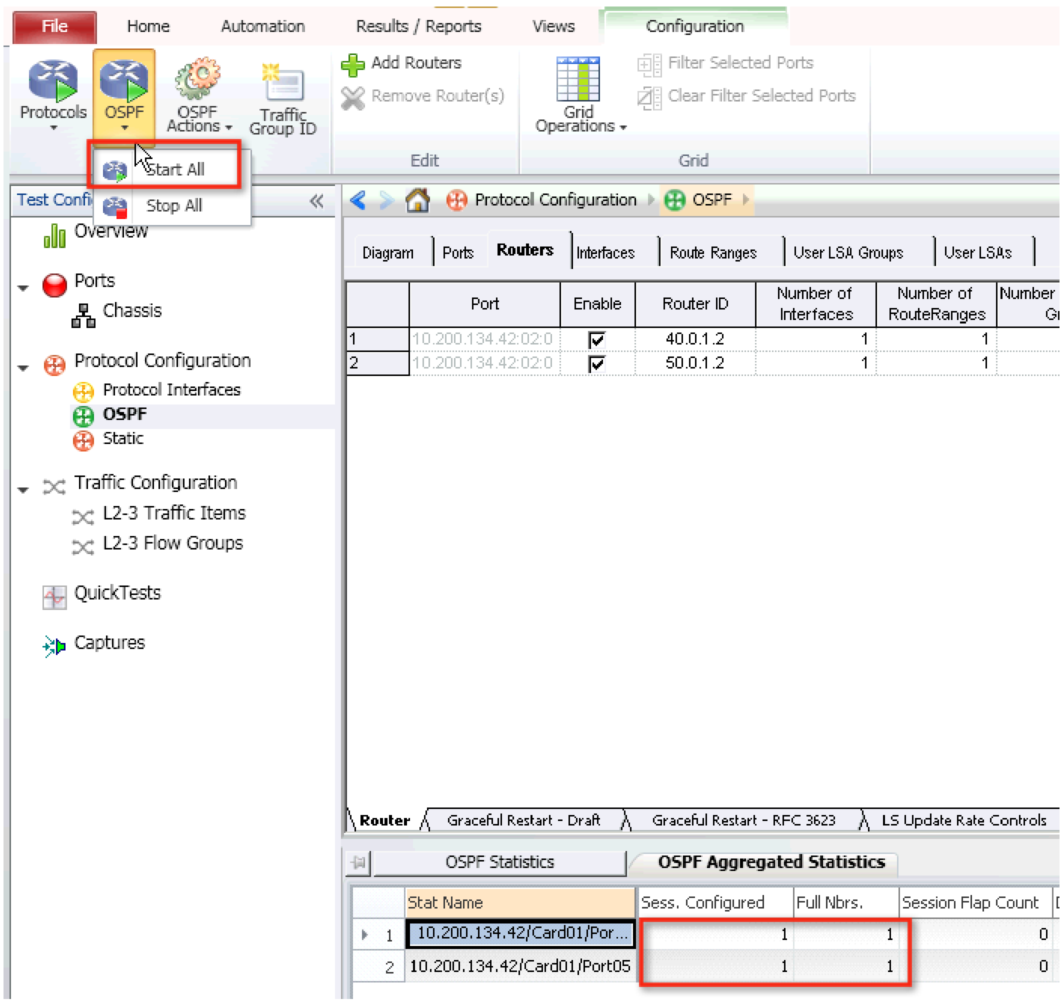


Figure 16. OSPF protocol statistics window

16. Once the OSPF sessions are up, enable **Convergence Mode** measurement. To enable Convergence Mode, do the following:

    a. Go to **Traffic Tools** > **Configuration** > **Traffic Options**.
    b. Select **CP/DP Convergence**.
    c. Select **Control Plane Events**. This option enables monitoring of control plane events. Based on event triggers, IxNetwork captures the hardware timestamp on an event start and end.
    d. Select **Data Plane Events – Rate Monitoring**. This option enables monitoring the throughput rate on the receive port, and captures the hardware timestamp when this user-defined threshold is reached. Values are captured on the primary receive port and secondary receive port.

    Note. If this option is grayed-out and cannot be enabled, disable other enabled measurements in this tab (For example, latency)

17. Configure Data Plane Threshold. Setting this threshold defines the Rx throughput threshold which when exceeded or dropped below, captures the timestamp.

    Note. A 90% rate threshold is recommended for this setting.

    Optionally, enable the **Packet Loss Duration** statistic. This IxNetwork statistic calculates the estimated time in milliseconds during which no packets were received for any traffic statistic view. This is calculated using **Frames Delta, Frame Size** and the **Tx Rate**.

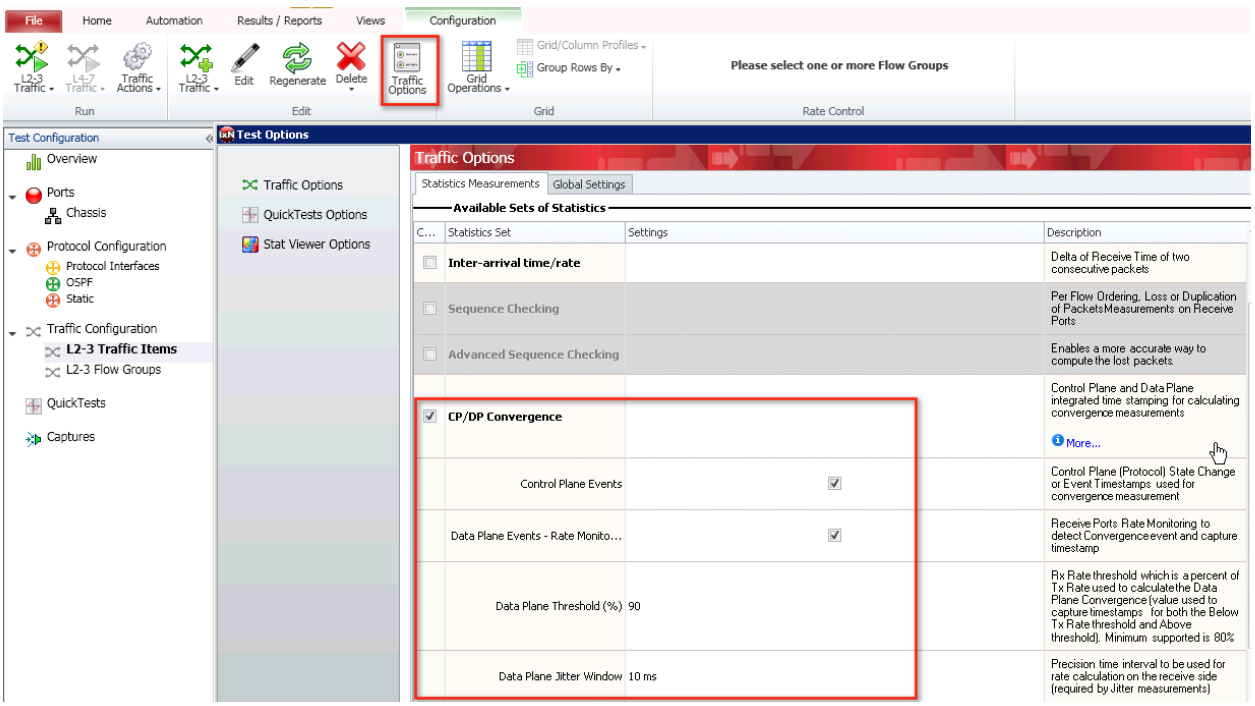


Figure 17. Enable Traffic options for convergence

18. Configure appropriate **Data Plane Jitter Window**. The jitter window is designed to avoid data plane jitter that can incorrectly trigger threshold timestamp. It is essentially the sampling period used to determine the incoming throughput on the monitored traffic flows. IxNetwork requires the minimum of 200 packets within each sampling period. The lower the value for data plane jitter window, the higher resolution and accuracy for DP threshold timestamps.

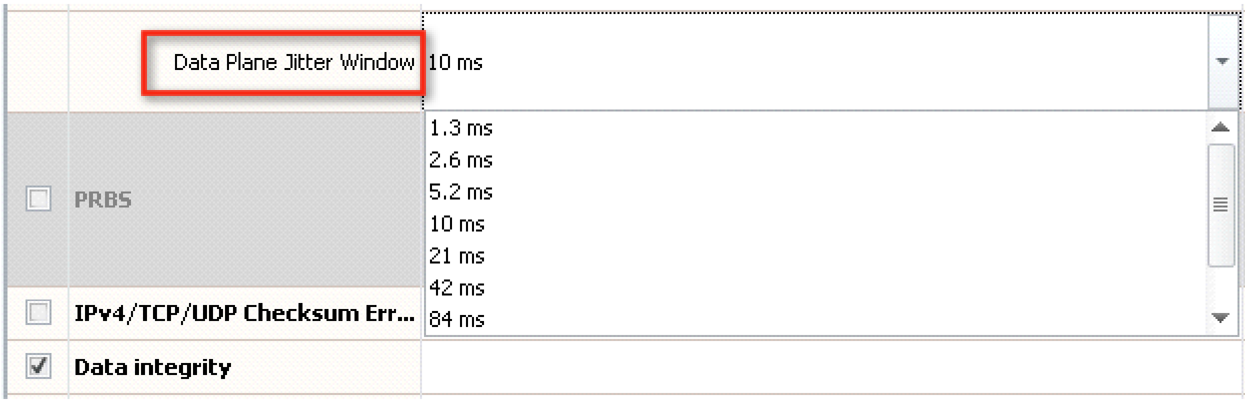


Figure 18. Select Appropriate 'Data Plane Jitter Window

19. Build traffic from the Traffic Port to the Primary Receive Port and Secondary Receive Port.

    a. Click **Traffic Tools** > **Configuration** > **L2-3 Traffic** to start the **Advanced Traffic Wizard**.

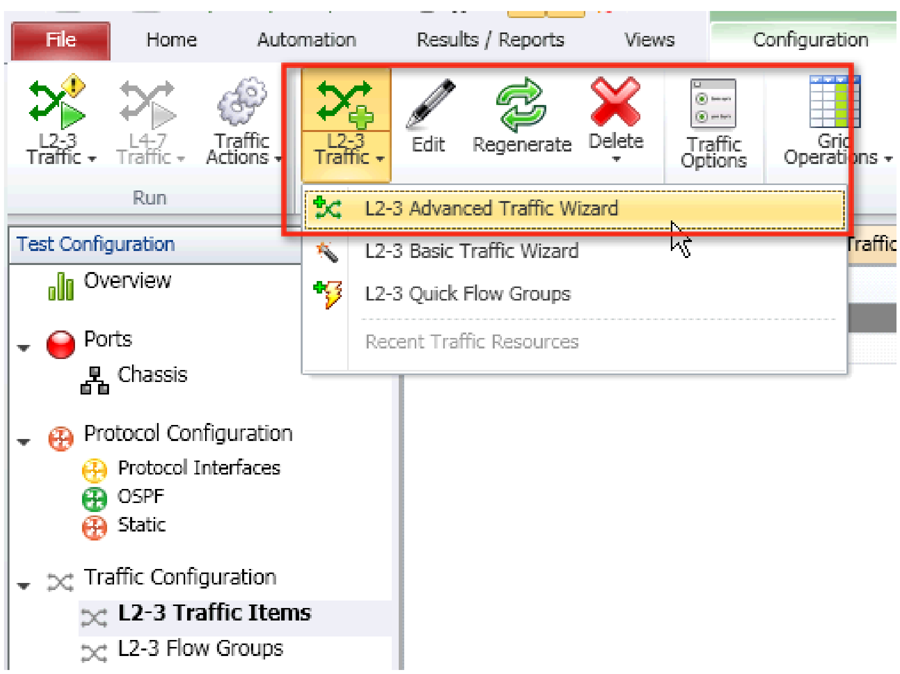


Figure 19. Create traffic

20. Once started, configure traffic. In the **Endpoints** pane, leave the defaults for **Source/Dest. Traffic Mesh** (*one-to-one*), **Routes/Hosts** (*one-to-one*), **Bi-directional** (*cleared*), **Allow Self-Destined** (*cleared*)

a. Set **Source Endpoints** as the protocol interface for the traffic port.
b. Set **Destination Endpoints** as the overlapping OSPF route ranges on the emulated OSPF routers on the primary receive port and the secondary receive port.
c. Click **Next.**

Note. The traffic is destined to overlapping IP address ranges (the same route range is advertised by both OSPF routers). So, IxNetwork automatically understands this is a convergence test and generates a single traffic stream. The path chosen to the destination is now decided based on the forwarding table on the DUT.

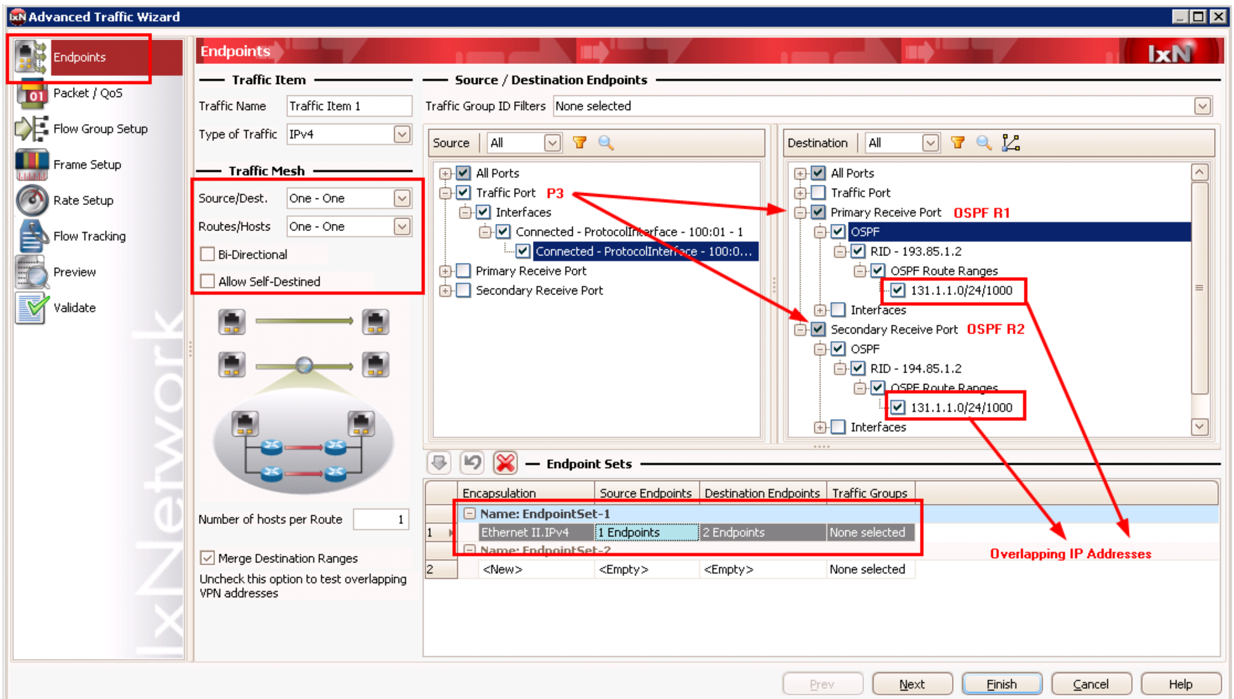


Figure 20. Advanced Traffic wizard (screen 1 - endpoints)

21. Optionally, in the **Packet/QoS** pane:

a. Available QoS fields are populated based on the traffic encapsulation. You can modify any available QoS field (For example, **IP Precedence**). Leave the default setting for this test.

22. Optionally, in the **Flow Group Setup** pane:

    a. Various options are populated based on packet content. These options allow you to create various traffic profiles that tune transmit parameters for each profile. Leave the default setting of *None* for this test.

23. Optionally, in the **Frame Setup** pane:

    a. Set the desired **Frame Size**.

24. Optionally, in the **Rate Setup** pane:

    a. Set the **Traffic Item Transmission Mode** to match the Transmit Mode in the Port Manager window.

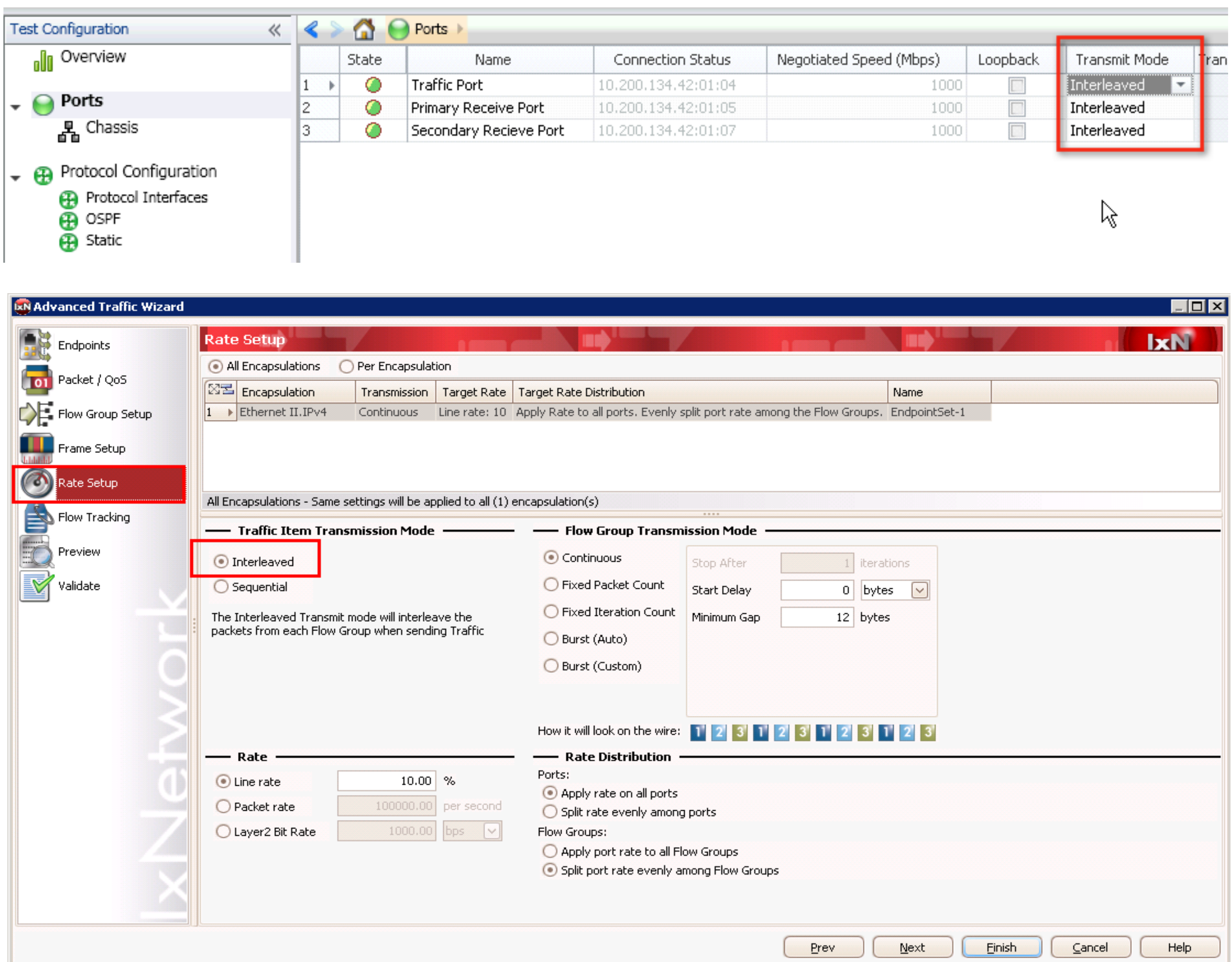


Figure 21. Advanced traffic wizard (screen 5 – rate setup)

25. In the **Flow Tracking** pane:

a. Select **Dest Endpoint** tracking. For convergence tests, this option MUST be selected. If this option is not selected, the traffic wizard displays a clear warning and the traffic apply fails.
b. Enable other tracking options if required.

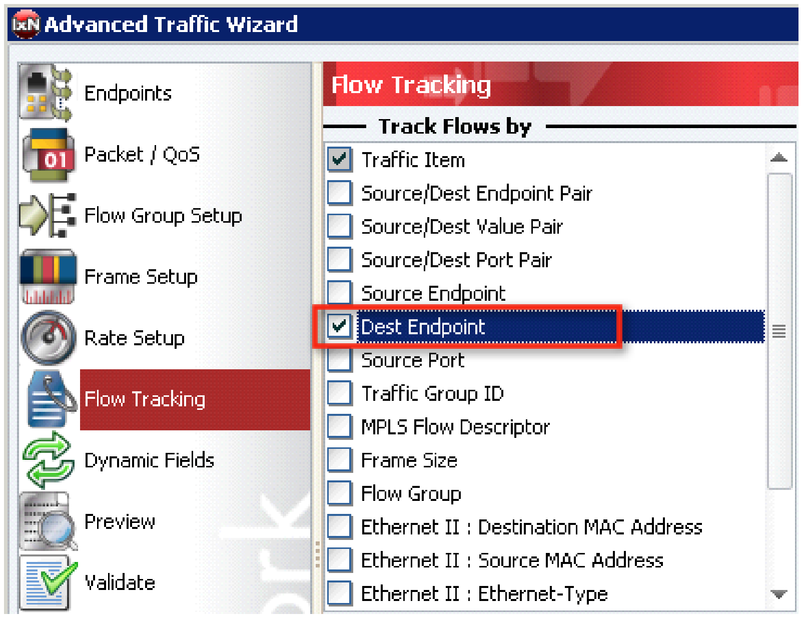


Figure 22. Advanced traffic wizard (screen 6 – flow tracking)

26. Optionally, in the **Preview** pane:

- Click View **Flow Groups/Packets** to preview the packet content.

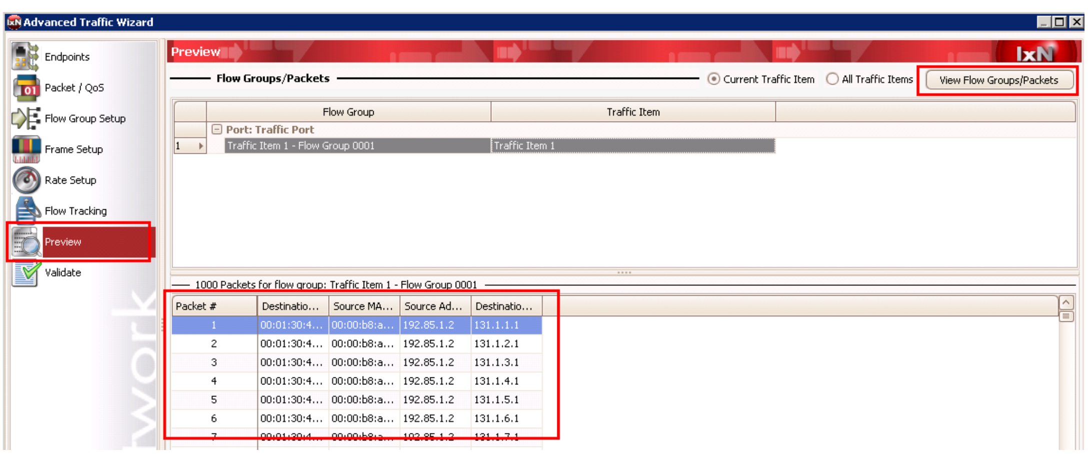


Figure 23. Advanced traffic wizard (screen 7 – preview)

27. Optionally, in the **Validate** pane:

    - Click **Validate** to ensure there are enough hardware resources to successfully build and apply traffic.

    Note. If traffic validation fails, a clear error is reported and details on how to correct the error are shown.

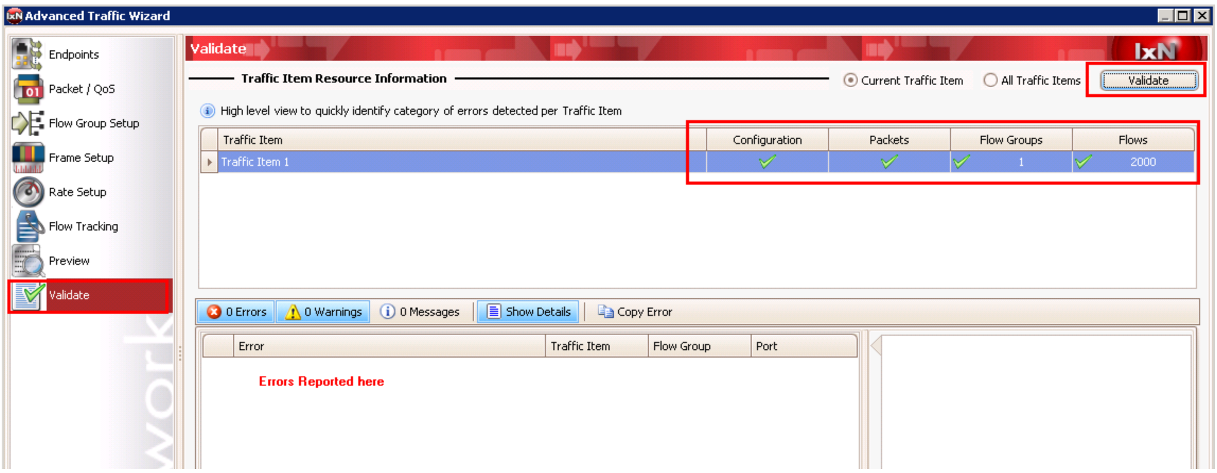


Figure 24. Advanced traffic wizard (screen 8 – preview)

28. Click **Finish**.

29. Once the Traffic wizard run is complete, traffic is built and a traffic item is created under the **L2-3 Flow Groups** node in the left pane. All flow groups for this traffic item show in traffic grid.

    - You can then dynamically modify the properties such as, **Frame Rate** and **Frame Size** for each flow group in the traffic grid.

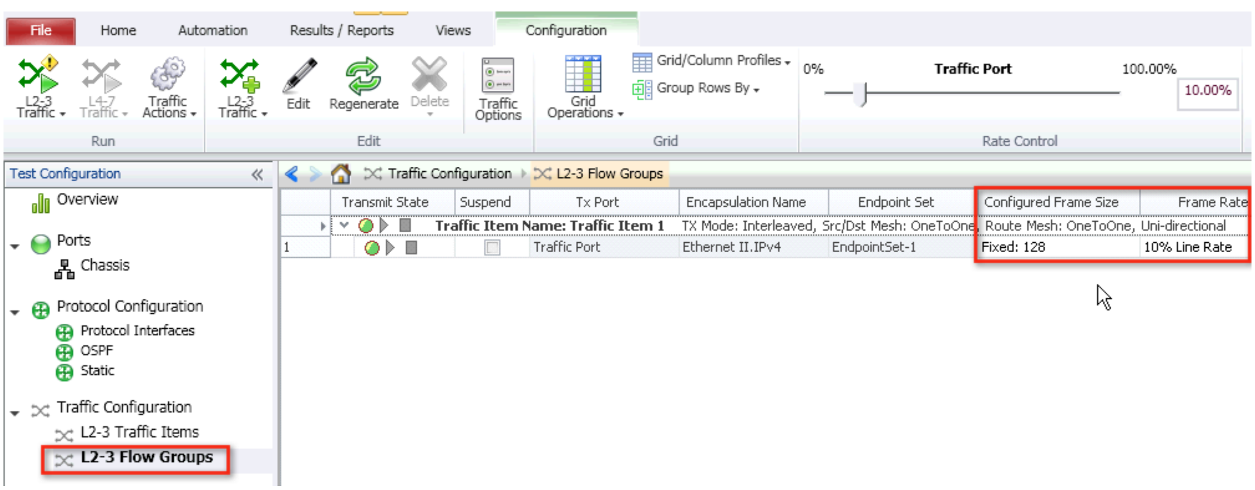


Figure 25. Traffic grid

30. View, **Apply,** and **Start** the traffic.

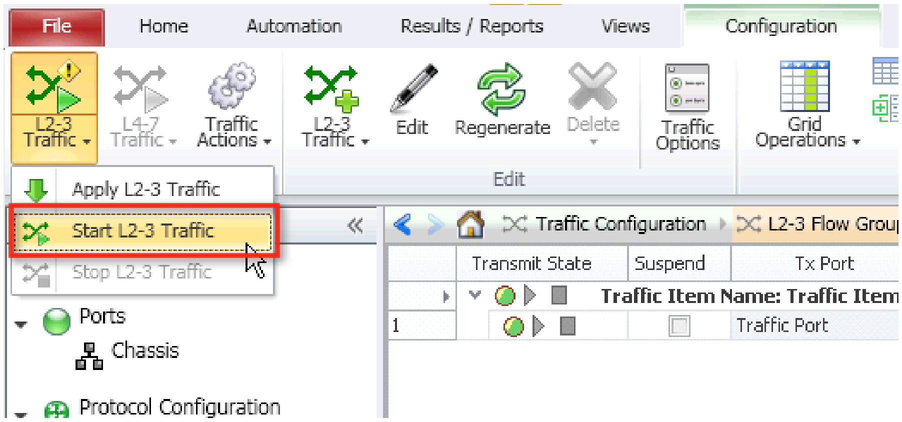


Figure 26. Traffic-created grid view

31. Click **L2-3 Traffic Items** > **Traffic Item Statistics** to view the traffic statistics.

- View the aggregated **Traffic Item Statistics**. This view is an aggregated traffic statistics view, per traffic item, and reports real-time loss, latency, and rate statistics for all ports in the traffic Item. This view does not include any convergence statistics.

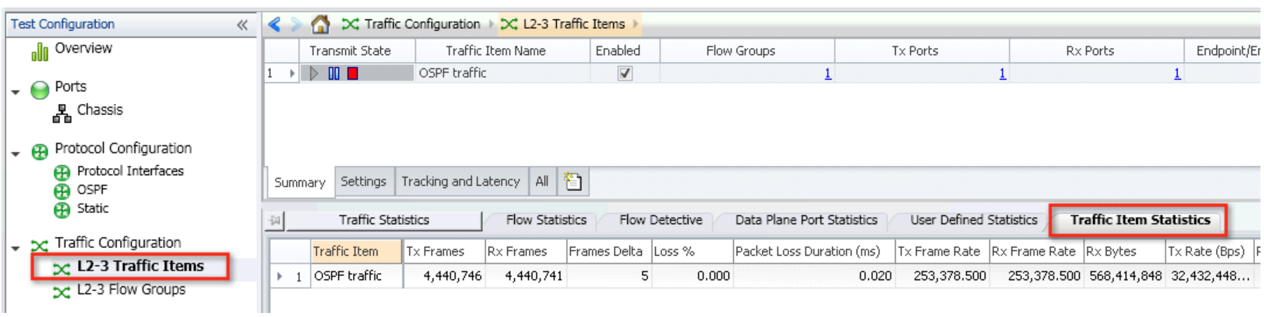
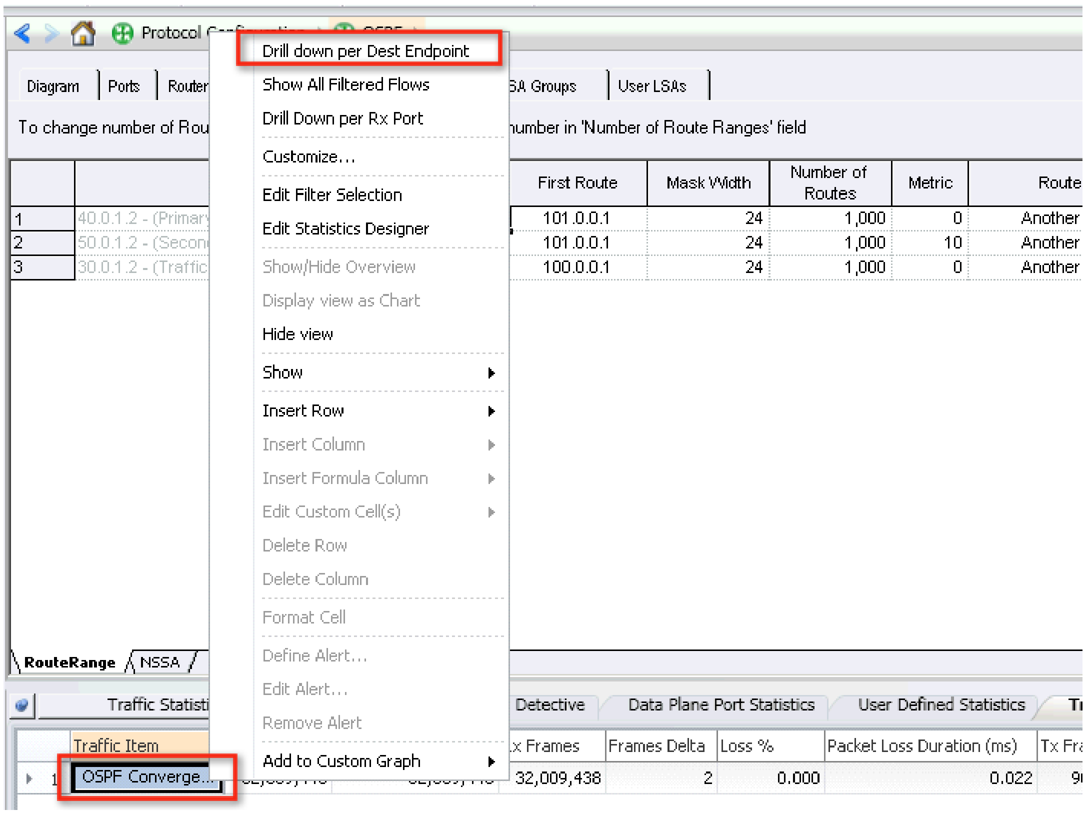


Figure 27. Aggregated traffic item statistics

32. Drill-down from the aggregated **Traffic Item View** to the **User-defined Statistics** view.

- Drill-down by **Dest. Endpoint** (right-click menu option from a selected traffic item. This is an aggregated view per advertised destination endpoint. This view contains:
    - CP/DP convergence time
    - DP/DP convergence time

  Ignore the values here, because no event triggering convergence has occurred. **Note**: The drill-down options per Traffic Item depend on the tracking options selected for that Traffic Item during configuration.



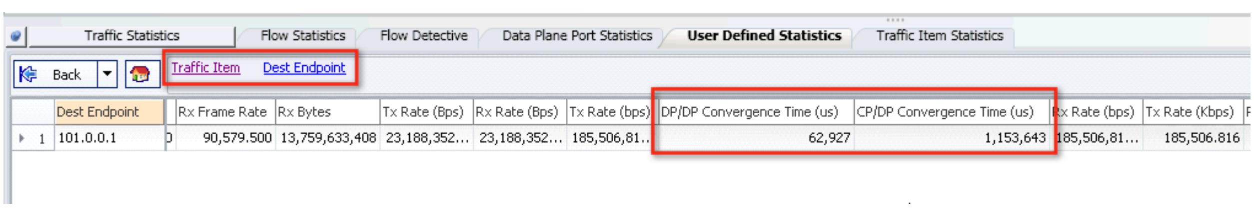


Figure 28. Drill-down view (user-defined statistics) per Dest. endpoint

33. Perform a second-level drill-down from the **Dest. Endpoint** view.

   a. Drill-down by **Rx Port** (right-click menu option from **Dest. Endpoint** view).
   This view is per-advertised destination endpoint and per-Rx port. This view contains:
   - Ramp-down Convergence Time (in microseconds)
   - Ramp-up Convergence Time (in microseconds)
   - Event Name
   - Event Start Timestamp
   - Event End Timestamp

   Ignore the values here, because no event triggering convergence has occurred.

   b. In the present view, the **Secondary Receive Port** is highlighted in blue, because it is **dead** and is not receiving any traffic.

   Presently all traffic is being received by the primary receive port, because it has the preferred path to the destination.

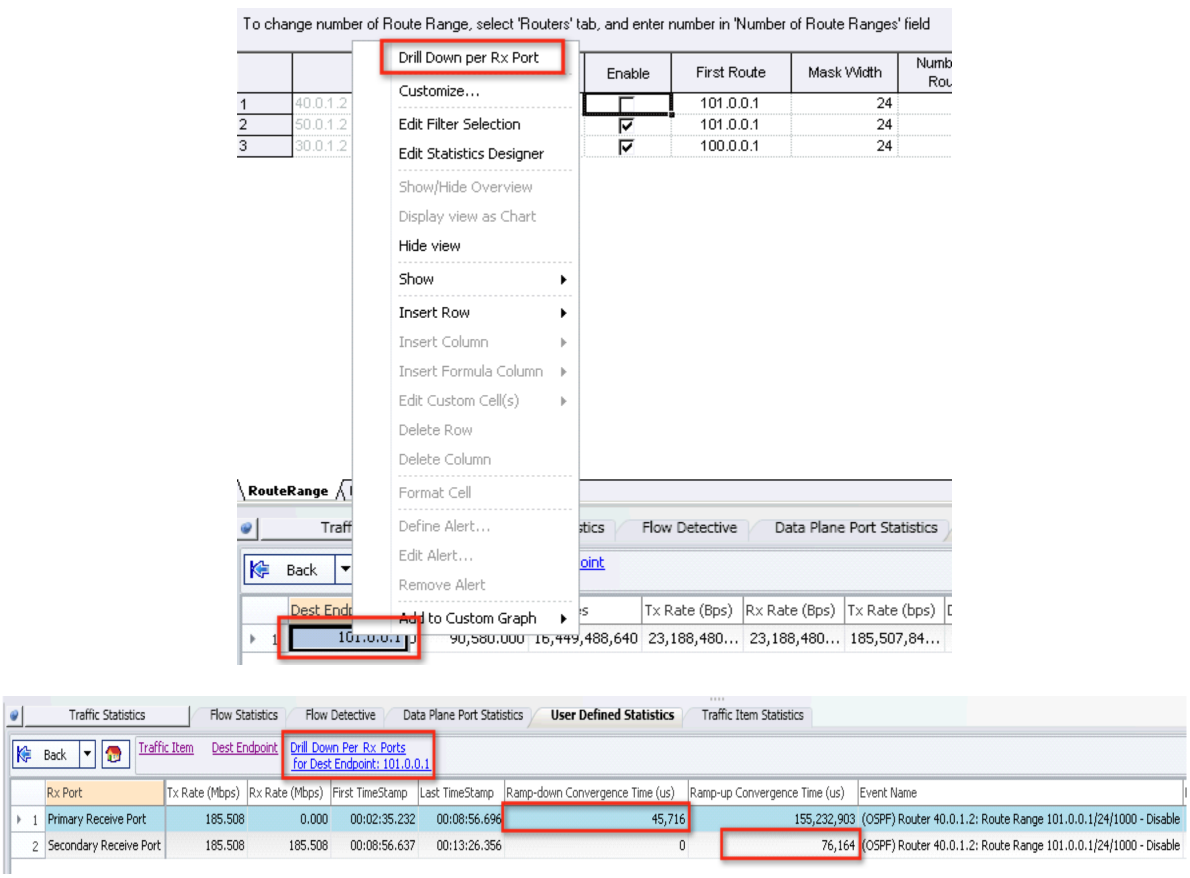


Figure 29. Drill-down view (user-defined statistics) per Dest. Endpoint, per Rx port

34. Trigger OSPF routes withdraw for convergence to occur. To trigger OSPF route withdraw, do the following:

    a. Navigate back to the **Protocol Configuration > OSPF** node in left panel.
    b. Click the **Route Ranges** tab.
    c. Clear the **Route Range** on the emulated OSPF router on the primary receive port. This action triggers convergence of all traffic being received on primary receive port to the secondary receive port as the DUT now uses the secondary path for all traffic destined to the route ranges.

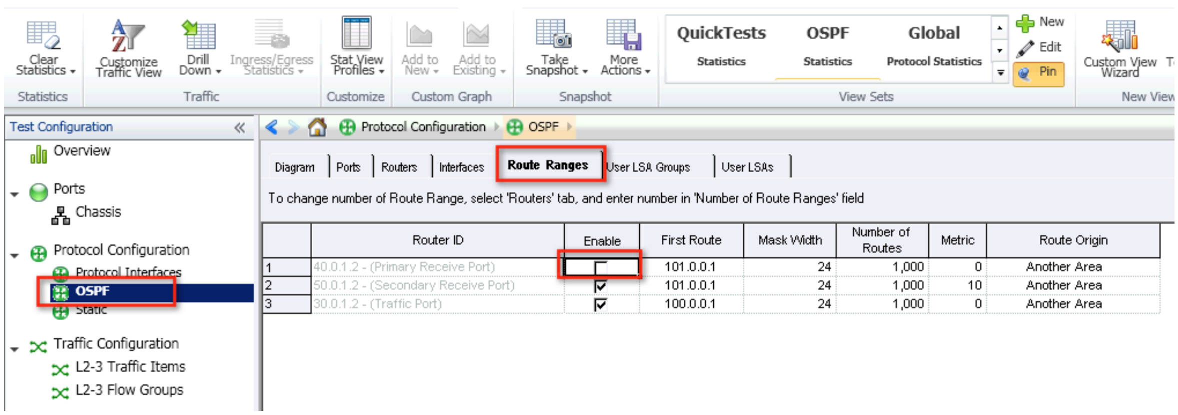


Figure 30. Disable OSPF route range on primary receive port

35. Navigate back to the **Traffic Statistics** tab.

36. Navigate back to the **Per Dest Endpoint Per Rx Port** view (Follow steps in Step 21). In this view, you notice that the primary receive port is dead, because it no longer receives the traffic. The secondary receive port is now receiving traffic and is no longer dead.

37. View the calculated values for the **Ramp-down Convergence Time**, **Ramp-up Convergence Time**, **Start Event Name**, **Start Event Timestamp**, and **End Event Timestamp**.

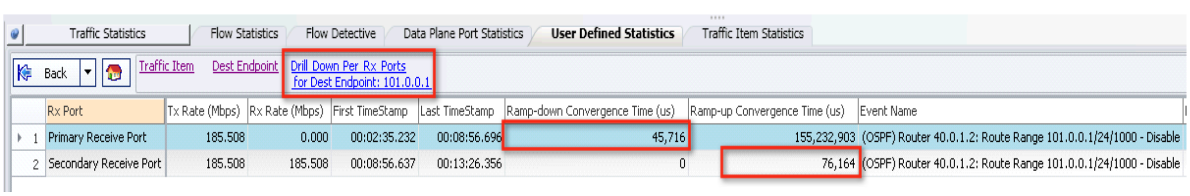


Figure 31. Ramp up/down convergence times

Note: The Ramp-up/down convergence times also take into account the amount of time taken for the completion of the event (OSPF route withdraw in this case), because the ports can completely Ramp-up and down only when all routes are withdrawn.

38. Navigate back to the **Per Dest. Endpoint** view (perform step 21, or navigate back from the previous view). In this view, you can see the calculated values for the **CP/DP Convergence time** and the **DP/DP Convergence time** (in microseconds).

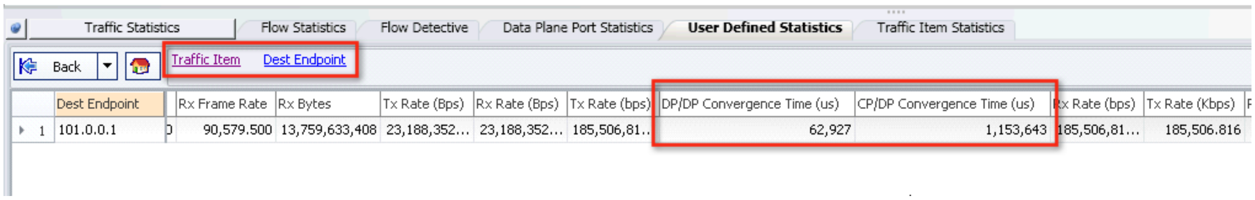


Figure 32. CP/DP and DP/DP Convergence times

Note: The **Flow Statistics** view reports the DP Above Threshold timestamp, DP Below Threshold timestamp and Event Start/End timestamp values for every flow in the test. The user can export these statistics to a CSV file and perform any additional calculations if needed.

About Service Interruption Time Measurement

When convergence occurs before reaching the last hop egress router, there can be temporary disruption of traffic flows on the same egress ports. IxNetwork is capable of two measurements to characterize such service interruption:

1. Packet Loss Duration – as described in step 17, this measurement is based on the amount of lost packets that represent the degree of service interruption. This methodology is less effective when the SUT (system under test) is capable of queuing/buffering packets and reducing the amount of lost packets.
2. Rate based monitoring – similar to route convergence measurement described in this test plan, DP-Below-Threshold and DP-Above-Threshold timestamps can be used to calculate Service Interruption Time (SIT).

The following steps describe how to use rate based monitoring to measure SIT:

a) Setup transmit traffic flows to target data paths that expect service interruption, due to convergence happing within system under test.
b) Setup RX flows monitoring through **Advanced Traffic Wizard** as described in step 25 to 28. Ensure the proper **Traffic Option** is selected, such as, **Data Plane Rate Monitoring**, **Data Plane Threshold**, **Data Plane Jitter Window**, as described in step 16 to 18.
c) Select **Flow Statistics**, define a new stats called SIT by Client Formula. Right-click any cell in **Flow Statistics**, and then click **Insert Formula Column**.

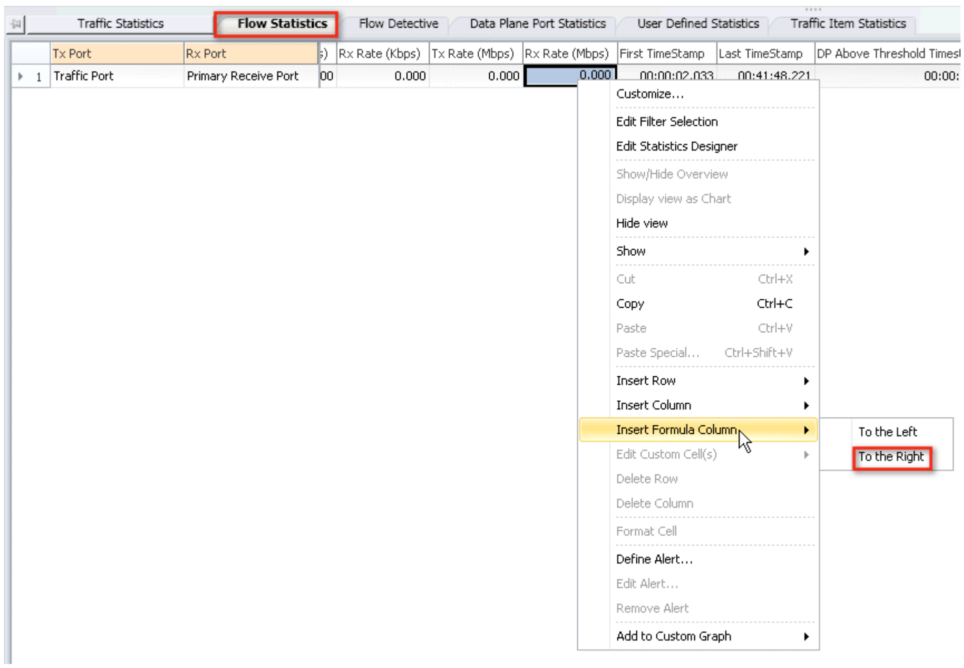


Figure 33. *Insert* Formula Column

d) Enter formula to calculate SIT.

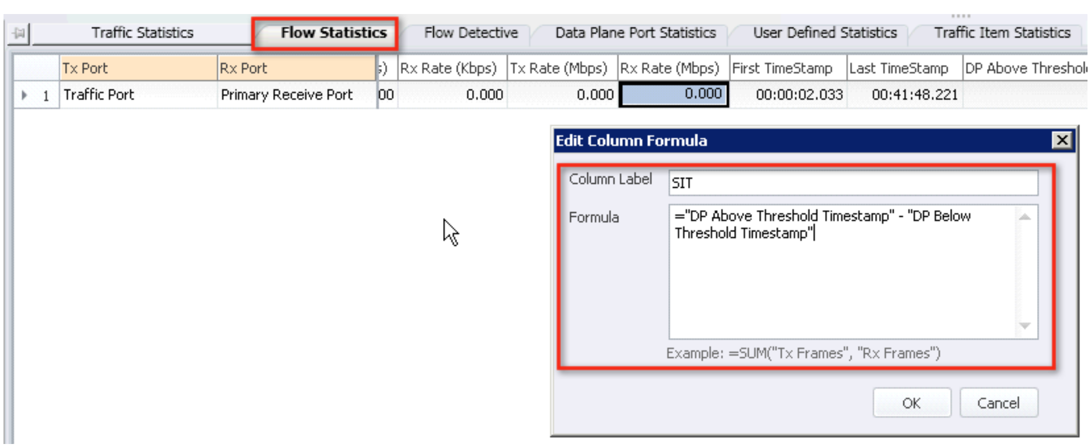


Figure 34. Define Service Interruption Time

e) Now the **Flow Statistics** is armed to measure SIT when the monitored throughput crosses the user defined threshold. The default value for **DP Above Threshold Timestamp** is zero, while the default value for DP Below Threshold Timestamp is the continuous update of last packet timestamp.

DP Above Threshold Timestamp	DP Below Threshold Timestamp
00:00:00.000	00:02:54.152

Figure 35. Default Values of DP above and below threshold timestamps

f) Once the monitored throughput are dropped below and restored above the threshold, both DP above and below threshold timestamps are latched to the fixed values and proper SIT will be displayed.

DP Above Threshold Timestamp	DP Below Threshold Timestamp	Service Int Time
00:44:23.183	00:44:22.401	00:00:00.782
00:44:23.183	00:44:22.401	00:00:00.782
00:44:23.183	00:44:22.402	00:00:00.781
00:44:23.183	00:44:22.402	00:00:00.781
00:44:23.184	00:44:22.402	00:00:00.781
00:44:23.183	00:44:22.402	00:00:00.781
00:44:23.183	00:44:22.402	00:00:00.781

Figure 36. Service Interruption Time Measurement

Note: Clear CP/DP statistics is needed to rearm the throughput threshold monitoring and set the Flow Statistics ready for next SIT measurement.

Results Analysis

The test constructed is a convergence test, where the triggering event for convergence was an OSPF route withdrawal. In this example, the protocol must withdraw each route and then the DUT must update the forwarding table with the new egress interface. The number of routes impacts the convergence time.

It is critical that devices capable of rapid convergence be tested across a myriad of different convergence-triggering scenarios. IxNetwork monitors a number of protocol and link events for TrueView convergence measurement. A detailed list of protocol events are available in the IxNetwork documentation.

Using Ixia's TrueView convergence and a simple workflow, the pre-defined convergence metrics provided by IxNetwork greatly reduce the amount of post-processing which is typically required in convergence test scenarios.

TrueView Convergence calculations

Measurement	Statistics Level
DP Above Threshold Timestamp	Flow Statistics
DP Below Threshold Timestamp	Flow Statistics
Control-Plane / Data-Plane Convergence Time	Destination Endpoint
Data-Plane / Data-Plane Convergence Time	Destination Endpoint
Event Name, Event Start Time, Event End Time	Flow Statistics Destination Endpoint -> Rx Port
Ramp Down Convergence	Destination Endpoint -> Rx Port
Ramp Up Convergence	Destination Endpoint -> Rx Port
Service Interruption Time	Flow Statistics, client formula required

Test Variables

The items listed in the following table are test cases for convergence. You can apply each variable to the test case set-up demonstrated above. By modifying a few parameters, you can create multiple tests validating the device performance under different failure conditions.

Control Plane Variables

Variable	Description
Change control plane protocol	**Step 4**: Change the control plane protocol being used in the convergence test. The same test methodology also applies to BGP routes convergence.
Change triggering event	**Step 22**: Change the event triggering convergence depending on the control plane protocol. Additionally, you can configure the event to be a link up/down event, which does not require any control plane to be configured.
Increase protocol scale	**Step 4**: Increasing Ixia OSPF routers per-port, the number of route ranges advertised, and/or number of routes per route range.

Data Plane Performance Variables

Performance Variable	Description
Change Data Plane Threshold	**Steps 16**: Manually change the data plane threshold setting to change the Rx rate being monitored.
Change Frame Size	**Steps 18/19**: Manually change the frame size of the traffic from the wizard, or dynamically from the traffic grid. Smaller frames typically cause more trouble for switches/routers. So tests run with 64-byte packets at a high frame rate yields worst case scenarios for convergence tests.
Increase Traffic Rate	**Steps 18/19**: Manually increase the rate at which traffic is sent from the wizard, or dynamically from the traffic grid.
Run test repeatedly	**Steps 14-23:** Automate all the convergence testing using the IxNetwork Event Scheduler, and run the test repeatedly to validate consistency in convergence times across multiple runs.

Troubleshooting and diagnostics

Issue	Troubleshooting Solution
Can't Ping from DUT	**Step 12**: Check the **Protocol Interface** window and look for red exclamation marks (!). If found, there is likely an IP address or gateway mismatch**.**
Sessions won't come up	**Step 15**: Go back to the **Test Configuration** window and double check the protocol configuration against the DUT. From the **Test Configuration** window, turn on **Control Plane Capture**, then start the Analyzer for a real-time sniffer decode between the Ixia port and the DUT port.
Convergence statistics values are very high while testing re-convergence	**Step 21/22/23:** While testing re-convergence (that is, validating convergence back from secondary to primary port (Preferred path coming back up)), select the **Clear CP/DP Stats** to clear all the Ixia hardware timestamps and get accurate convergence values. Failure to do this selection yields high and incorrect convergence values.

Test Case: BGP RIB-IN Convergence Test

Overview

The Border Gateway Protocol (BGP) is widely used to distribute reachability information to setup end-to-end IP services within and across AS boundaries. The ability of a router to restore BGP states/sessions, converge routes, and services following an unplanned service disruption is critical for service providers to ensure SLAs with confidence.

Draft-ietf-bmwg-bgp-basic-convergence defines several test cases to characterize BGP RIB (routing information base) and FIB (forwarding information base) performance, including:

- RIB-IN Convergence
- RIB-OUT Convergence
- eBGP Convergence
- iBGP Convergence
- BGP Hard/Soft Reset Convergence
- BGP Routes Withdraw Convergence
- BGP Path Attribute Change Convergence
- BGP Graceful Restart Convergence

Objective

The RIB-IN convergence test is designed to measure the convergence time required to receive and install BGP routes in Routing Information Base using BGP.

Setup

As defined in section 5.1.1 of draft-ietf-bmwg-bgp-basic-convergence, the definition of RIB-IN convergence (a.k.a FIB convergence) is described as following:

- R2 sends traffic toward BGP routes in AS 200
- R1 advertises BGP routes at RCV-Rt-time
- R1 receives traffic for BGP routes at DUT-XMT-Data-Time
- RIB-IN Convergence time = DUT-XMT-Data-Time - RCV-Rt-time

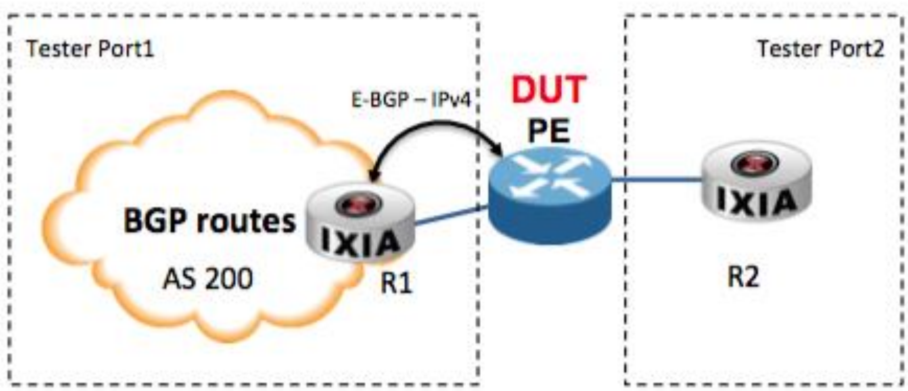


Figure 37. RIB-IN convergence test setup

Step-by-Step Instructions

The following instructions assist in creating a convergence test as shown in the Figure above. In addition, you can use these instructions as a guide for building many other convergence test scenarios.

1. Reserve two ports in IxNetwork.

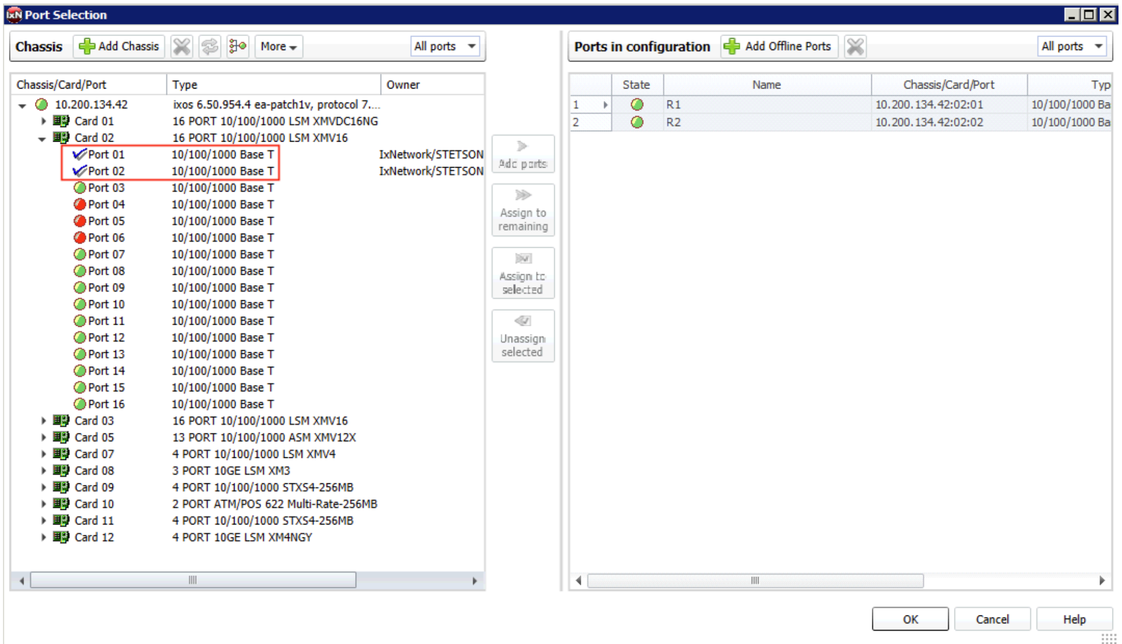


Figure 38. Port Reservation

2. Rename the ports as R1 and R2 for easier use throughout IxNetwork.

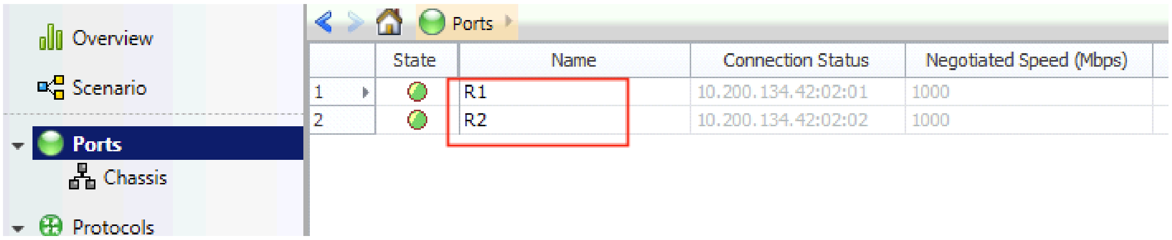


Figure 39. Port Naming

3. Click **Home > Add Protocols.**

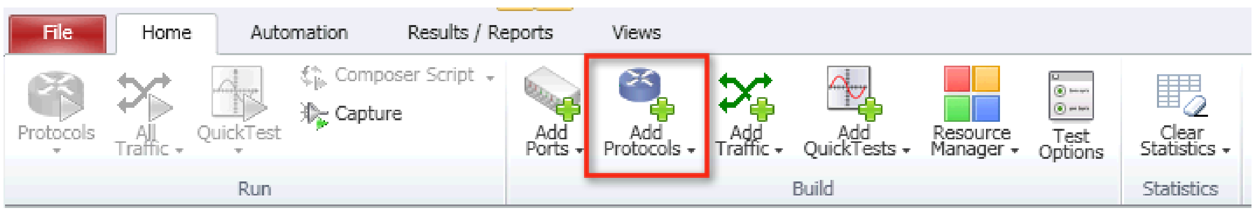


Figure 40. Protocol wizards

4. Run the **BGP** protocol wizard.

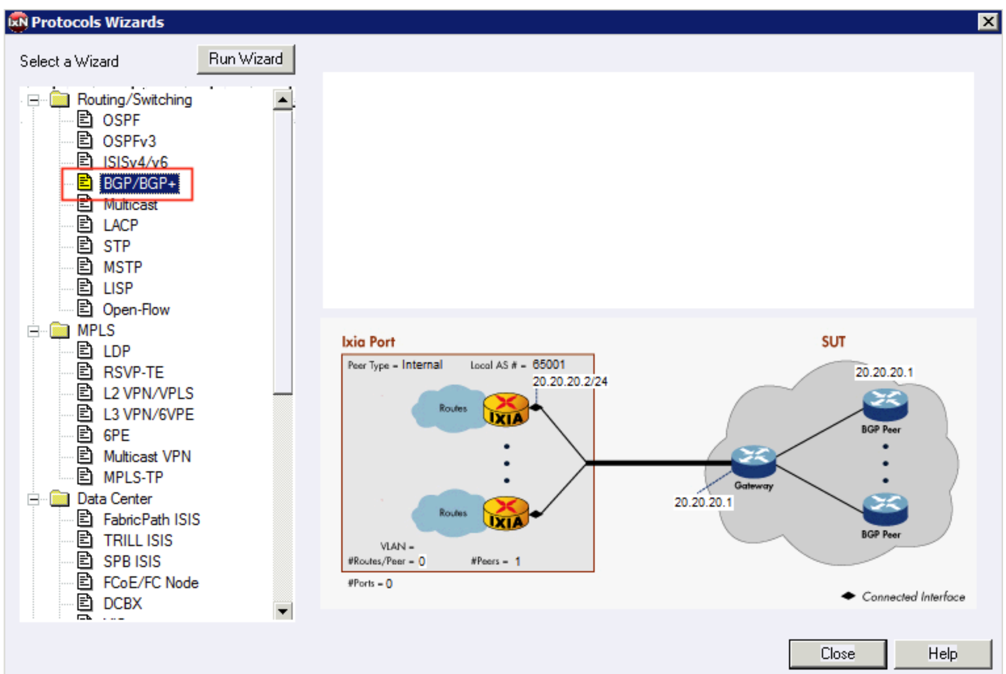


Figure 41. BGP wizard

5. Select port R1 for BGP wizard configuration. Click **Next** to continue the configuration.

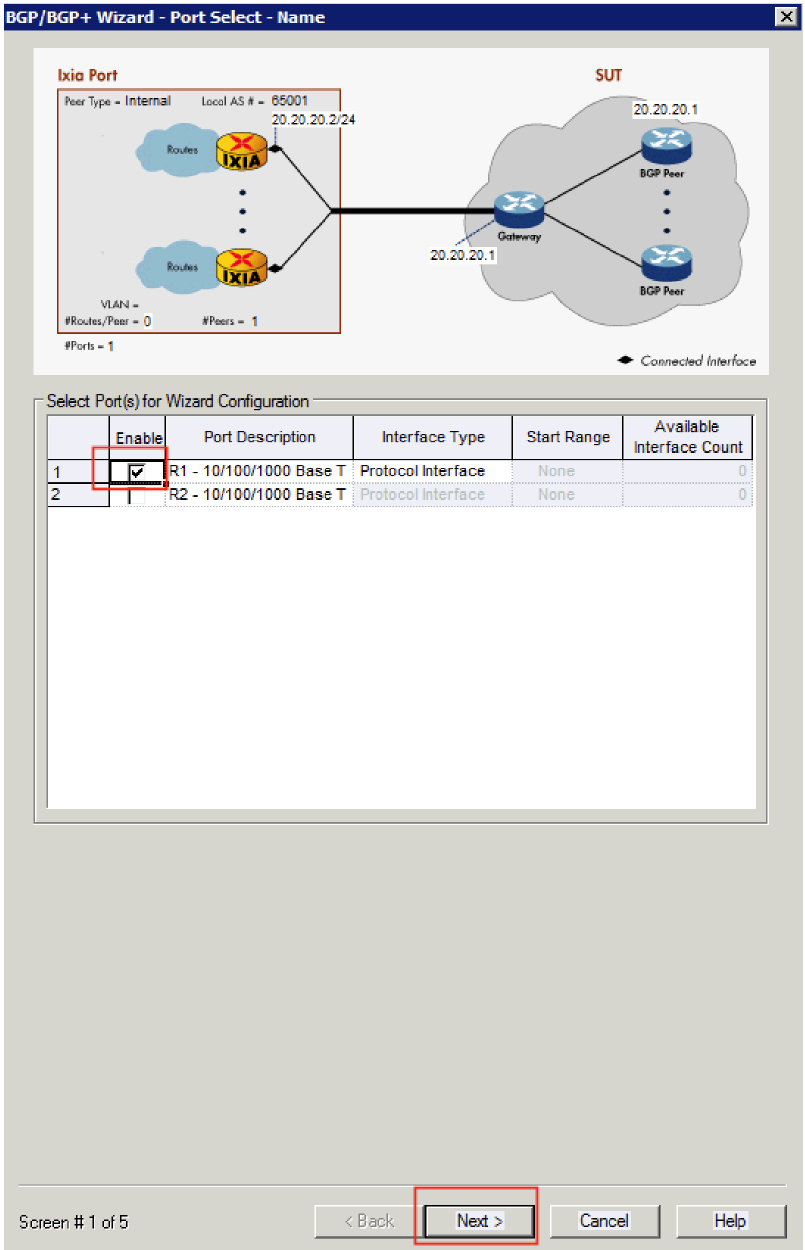


Figure 42. BGP wizard #1

6. Leave all parameters as default. Click **Next** to continue.

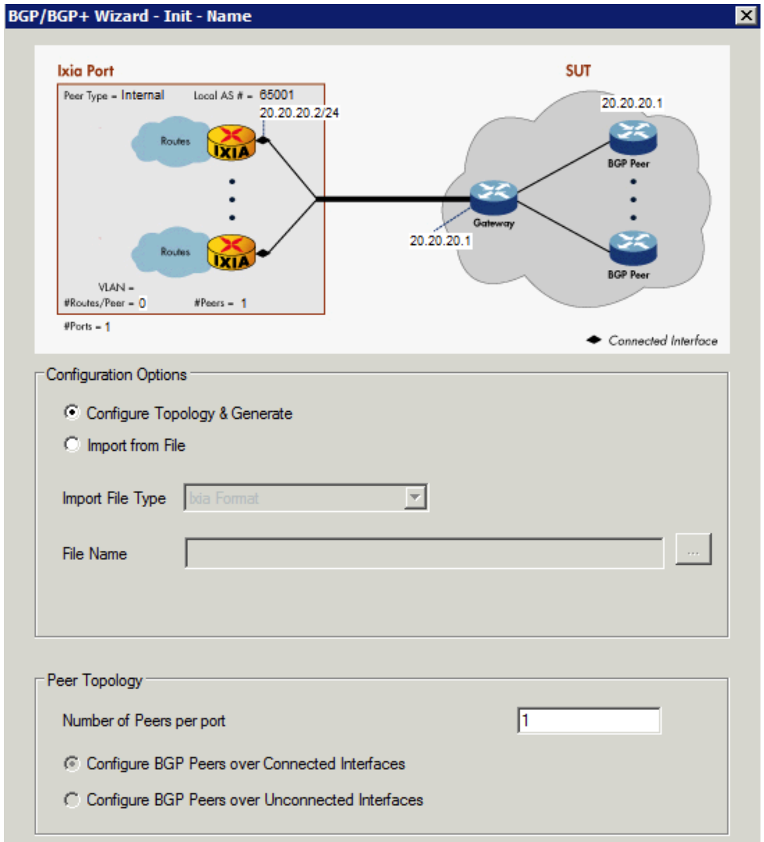


Figure 43. BGP wizard #2

7. Select **Enable VLAN** check box and enter relevant values. Similarly, enter appropriate value for **Emulated Peer IP Address.** Click **Next** to continue.

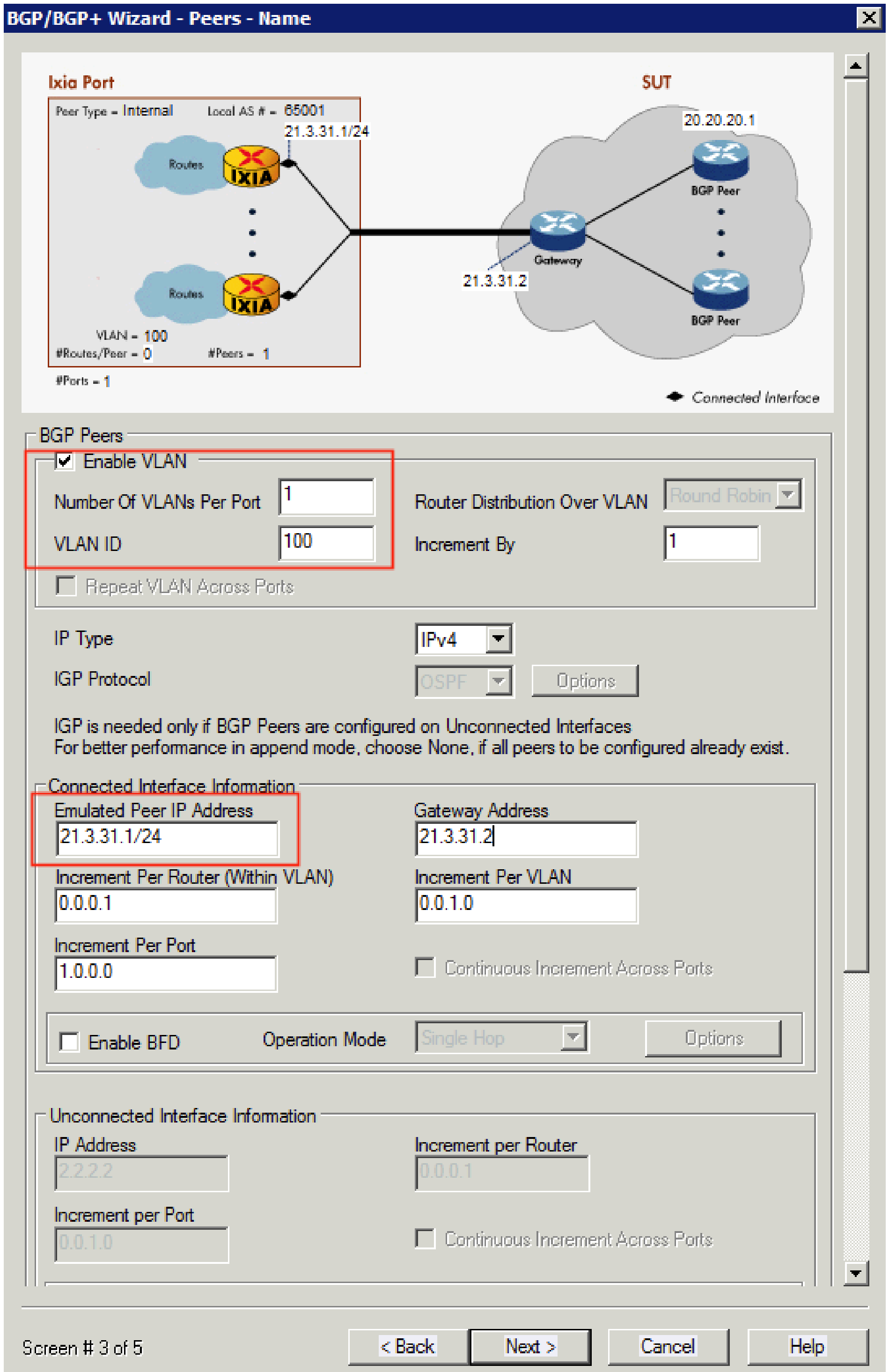


Figure 44. BGP wizard #3

8. Enter appropriate values for **BGP Type**, **Local AS Number Start**, and **Route Parameters** as depicted in the following image. Click **Next**.

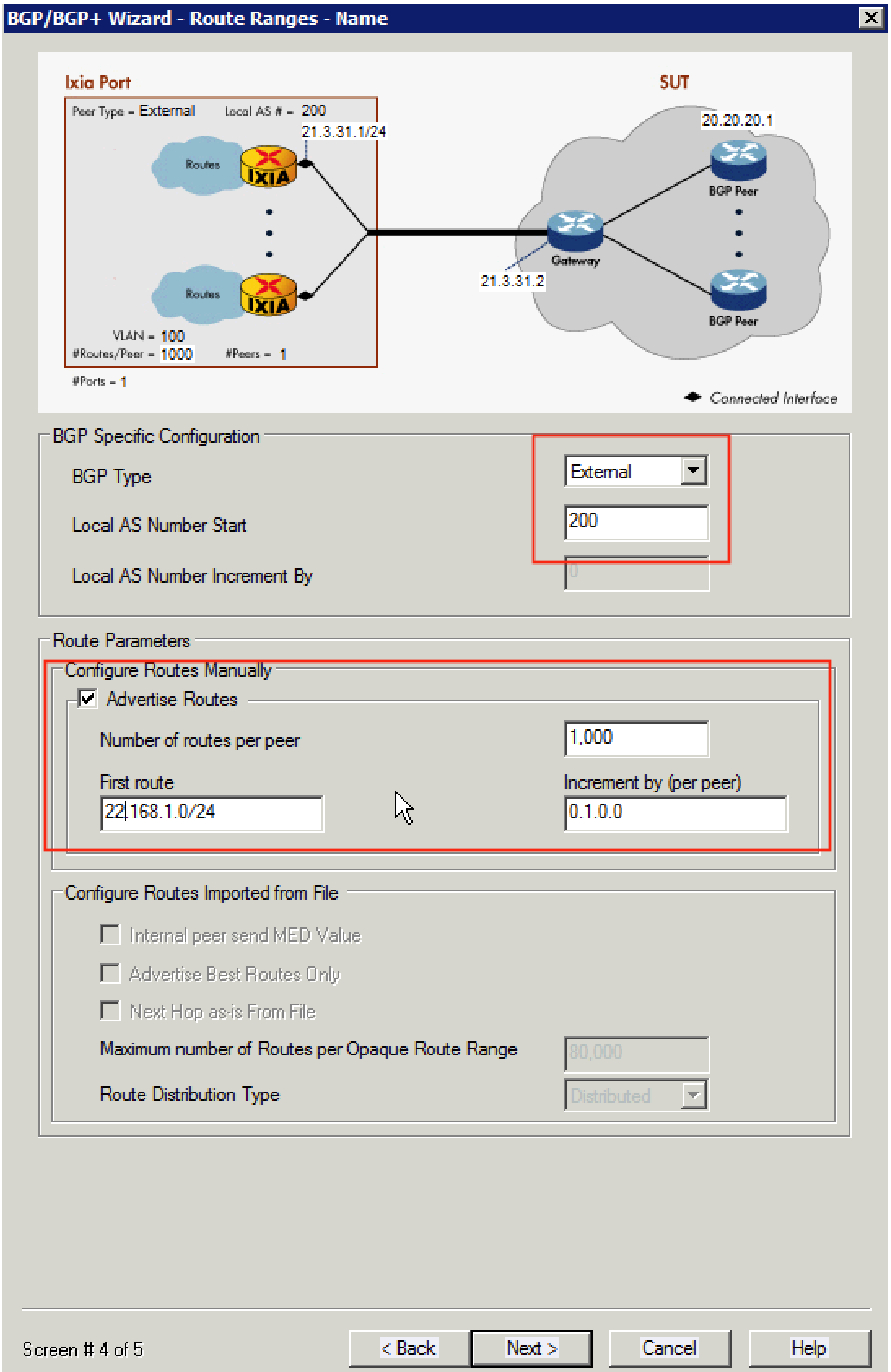


Figure 45. BGP wizard #4

9. Provide a name for this wizard. Click **Generate and Overwrite Existing Configuration**. Click **Finish**.

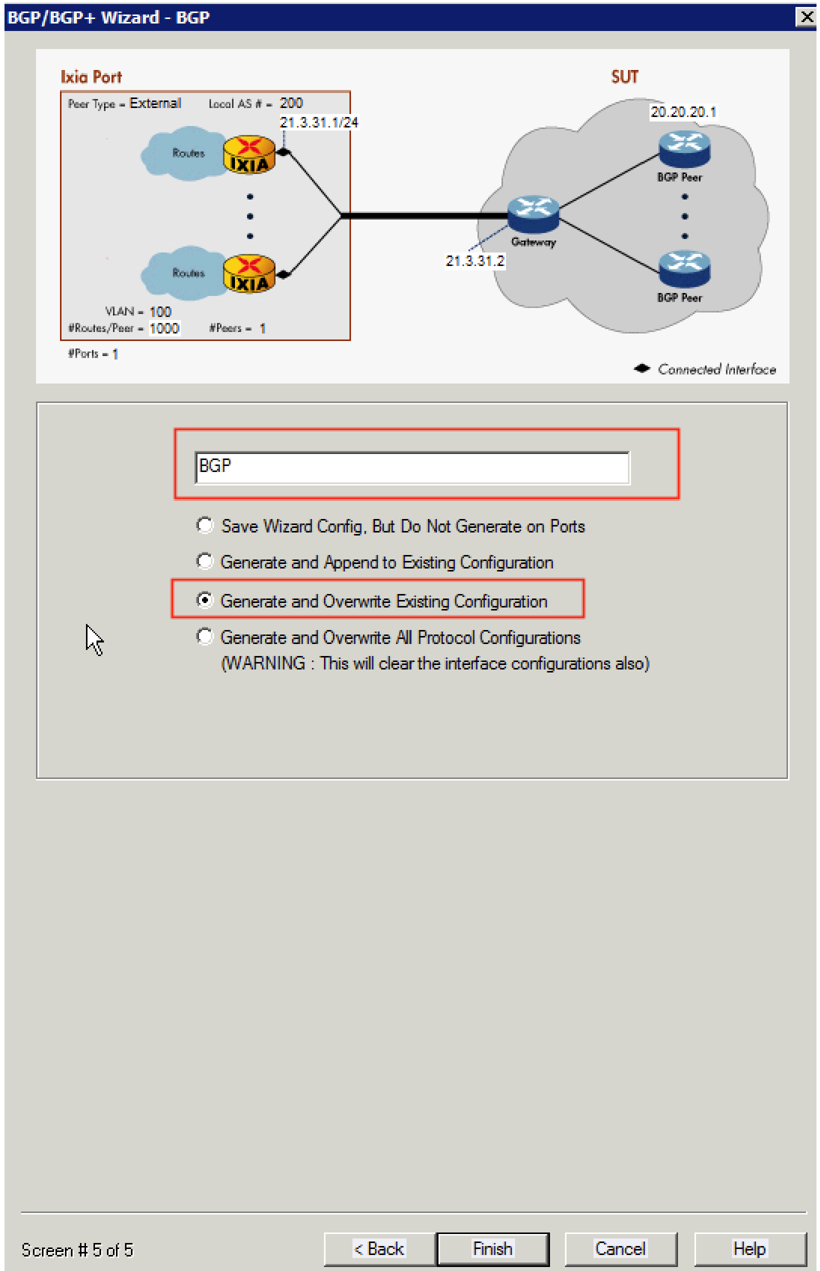


Figure 46. BGP wizard #5

10. Click **Protocols** to start up all protocol emulation.

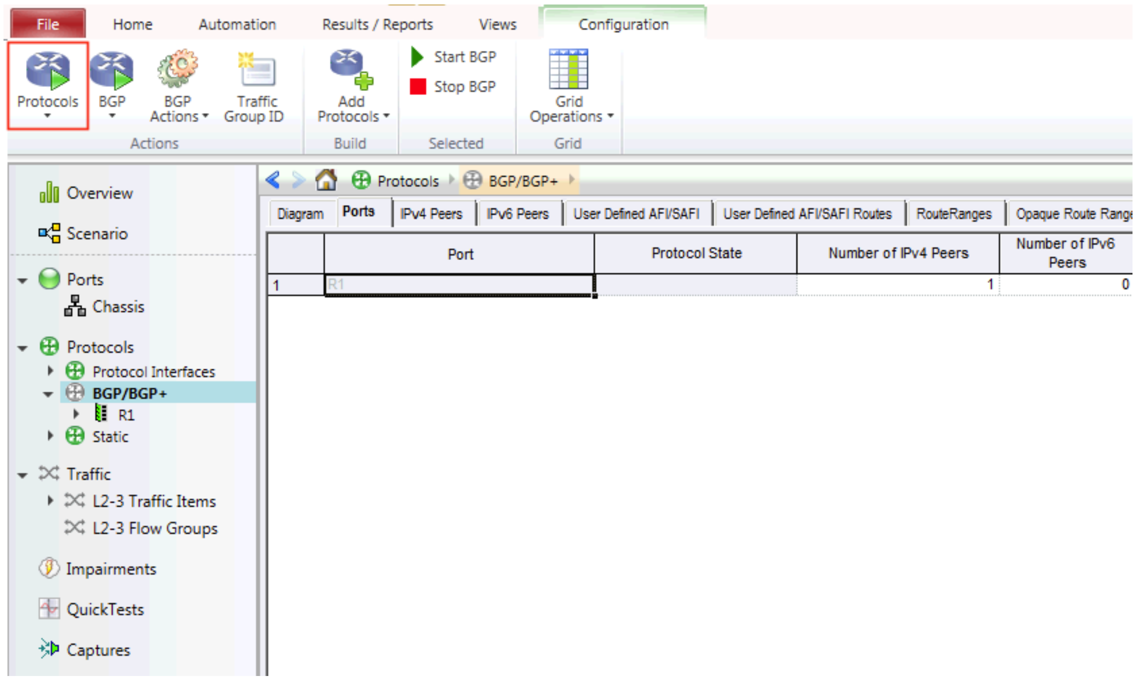


Figure 47. Start BGP protocol

11. Verify that the BGP session is up and running.

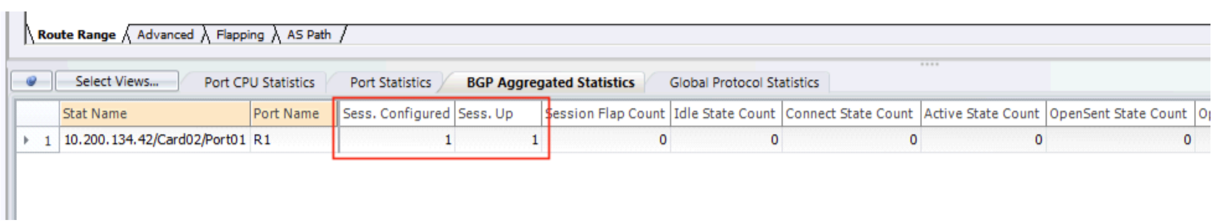


Figure 48. Verify BGP sessions

12. Follow steps 16, 17, and 18 in OSPF convergence test case to enable TrueView convergence measurement in traffic option.

13. Follow steps 19 through 30 in OSPF convergence test case to build up the test traffic. The source end point is the Connected IP interface of emulated R2 and the destination end point is the advertised BGP route range of emulated R1.

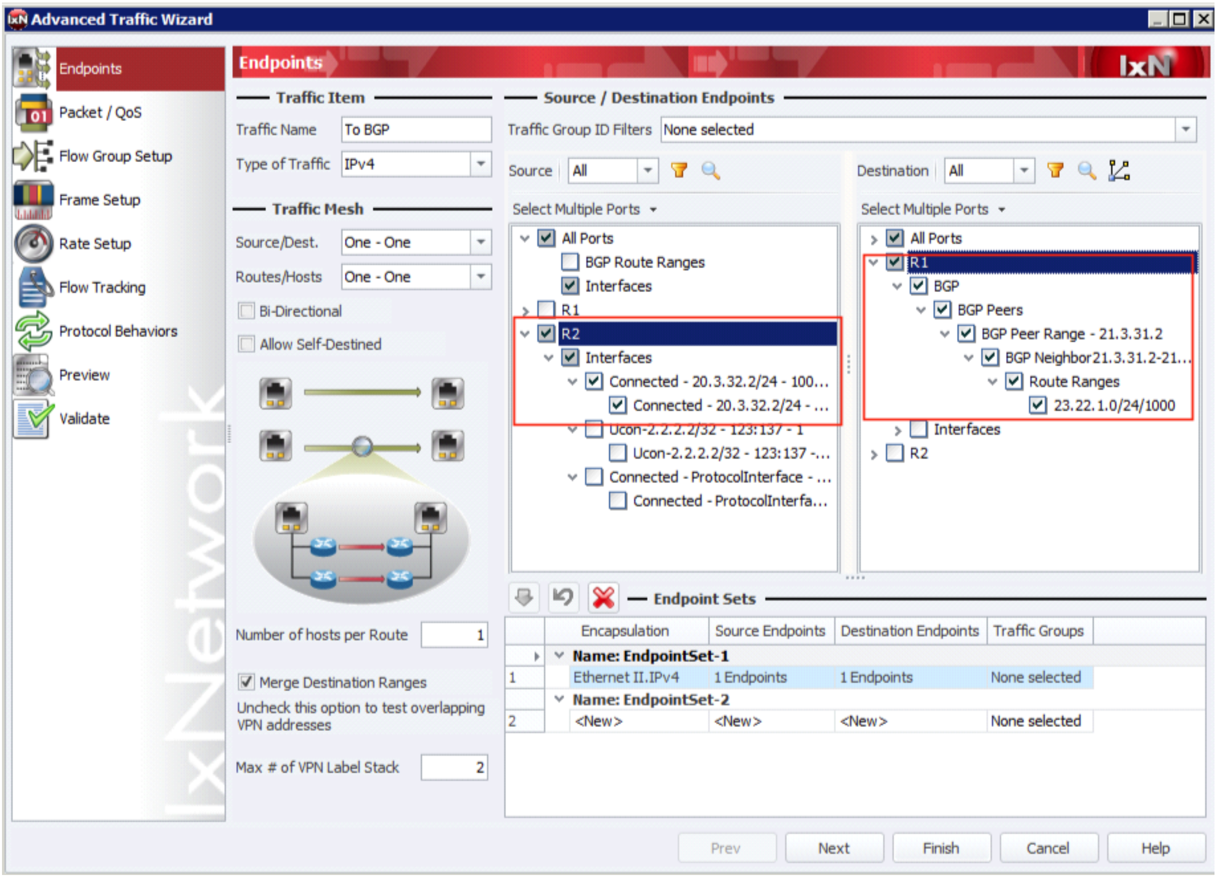


Figure 49. Traffic wizard config

14. View the traffic statistics (navigate to **L2-3 Traffic Items** > **Traffic Item Statistics**).

   a. View the aggregated **Traffic Item Statistics**. This view is an aggregated traffic statistics view, per traffic item, and reports real-time loss, latency, and rate statistics for all ports in the traffic Item. This view does not include any convergence statistics.

   b. Ensure that the DUT is not dropping packets with the configured traffic load before convergence measurement. If the packet loss is observed, reduce the traffic loading until no packet loss.

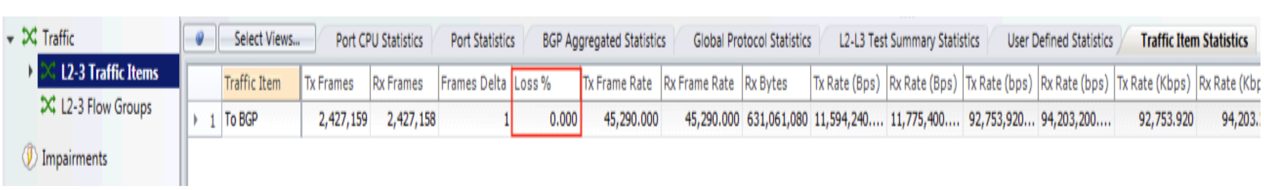


Figure 50. No traffic loss validation

15. In the left pane, click **BGP/BGP+**. Click the **RouteRanges** tab. Clear the **Enable** check box to disable the route range.

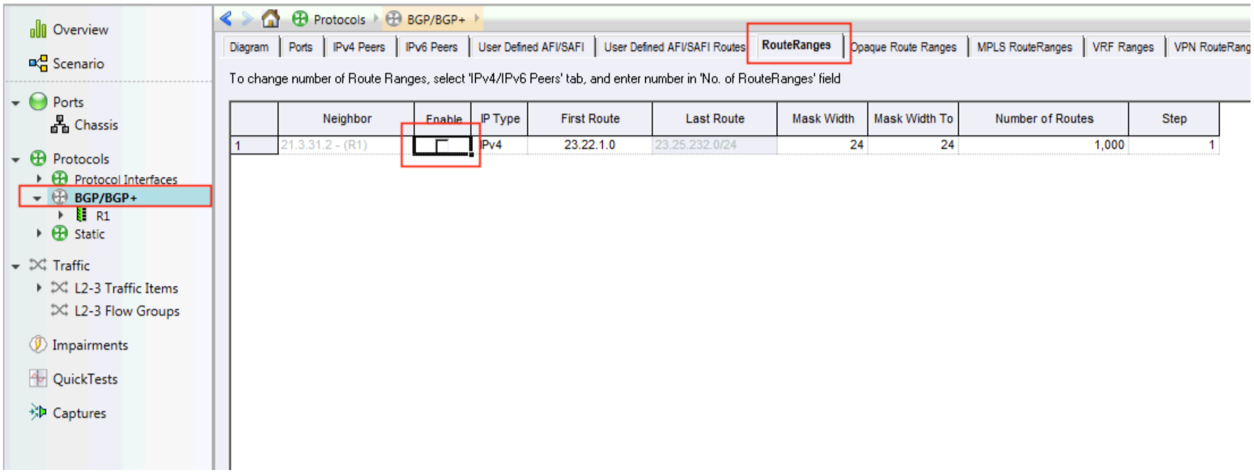


Figure 51. Uncheck BGP route range

16. Clear all traffic statistics before convergence measurement.

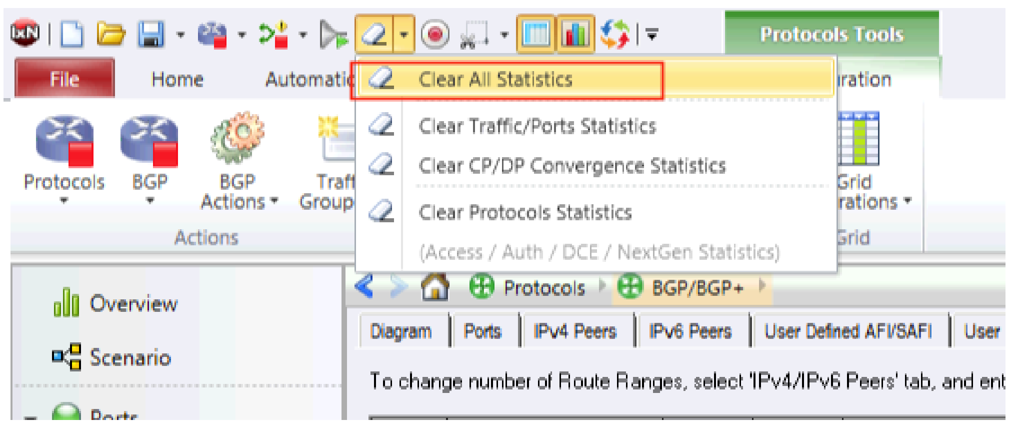


Figure 52. Clear all statistics

17. Drill-down from the aggregated Traffic Item View to the User-defined Statistics view.

 a. Drill-down by **Dest. Endpoint** (right-click menu option from a selected traffic item. This is an aggregated view per advertised destination endpoint. This view contains:

- CP/DP convergence time (equivalent to RIB-IN convergence)
- DP/DP convergence time (no valid in this test configuration)

 There is no occurrence of event triggering convergence. So ignore the values here. **Note**: The drill-down options per Traffic Item depend on the tracking options selected for that Traffic Item during configuration.

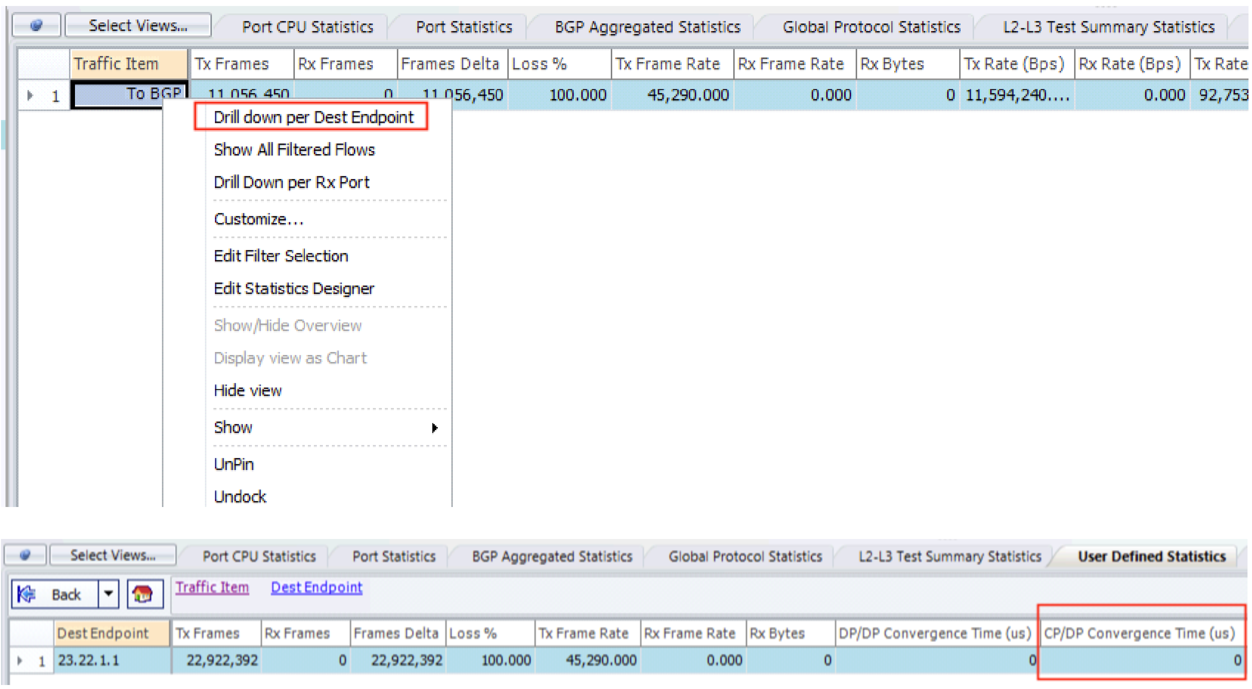


Figure 53. Drill-down view (user-defined statistics) per Dest. Endpoint

18. In the left pane, click **BGP/BGP+**. Click the RouteRanges tab. Advertise the 1000 BGP routes by selecting the enable box. Expect the 1000 routes to be installed in DUT and traffic forwarded by DUT.

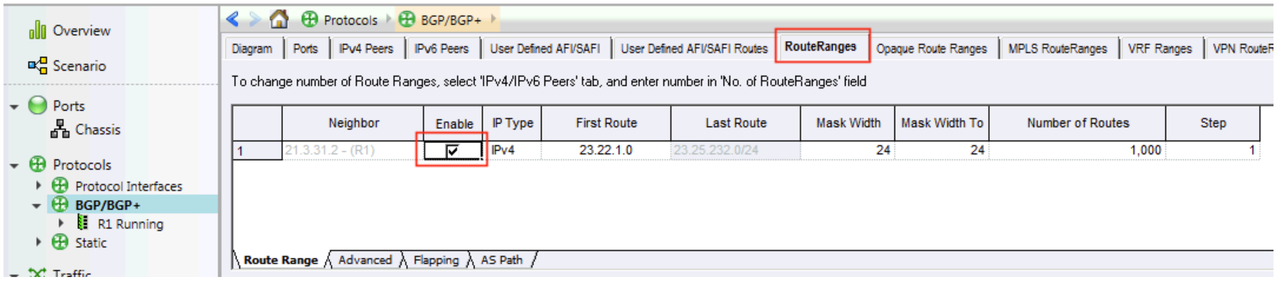


Figure 54. Advertise BGP routes

19. Select traffic item to analyze the traffic forwarded by DUT. Now the routes are installed in RIB. The DUT starts forward packets. Scroll to CP/DP convergence time in Dest Endpoint drilldown view. You must observe 155.618ms RIB-IN convergence time. By the definition of draft-ietf-bmwg-bgp-basic-convergence, RIB-IN convergence (also known as, FIB convergence) = CP/DP convergence in IxNetwork TrueView convergence measurement.

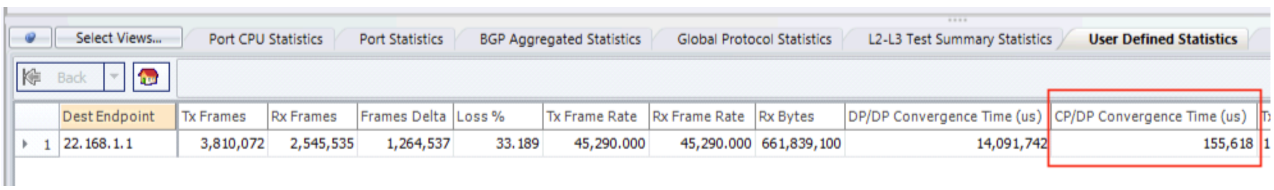


Figure 55. RIB-IN convergence

20. Optionally, user can repeat the RIB-IN convergence measurement by withdrawing the BGP routes at R1 router, clear CP/DP statistics as illustrated in the following figure, and then repeat the steps 17 and 18.

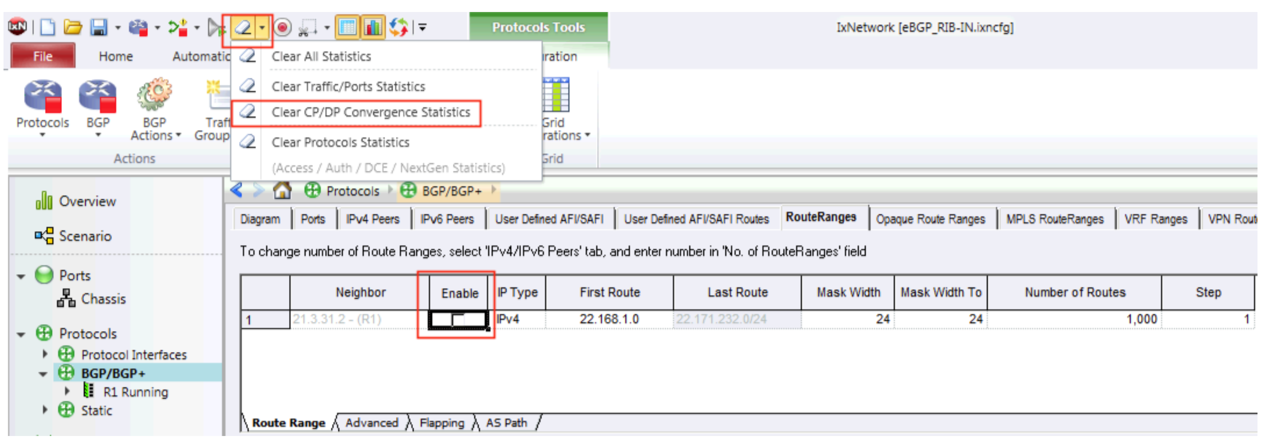


Figure 56. Clear CP/DP convergence statistics

Result Analysis

It is highly recommended to take multiple measurements and observe the average value and deviation. IxNetwork Test Composer is ideal for automating such iterated tasks. For example, the following results were automated in Test Composer with average convergence time and deviation:

Iteration	FIB/RIB In Convergence (ms)
1	286.0
2	293.0
3	289.0
4	249.0
5	267.0
Average	276.8
Deviation	15.0

Test Variables

As recommended by draft-ietf-bmwg-bgp-basic-convergence, vary the size of advertised routes in order to fully characterize DUT’s FIB convergence performance

Contact Ixia

Corporate Headquarters
Ixia Worldwide Headquarters
26601 W. Agoura Rd.
Calabasas, CA 91302
USA
+1 877 FOR IXIA (877 367 4942)
+1 818 871 1800 (International)
(FAX) +1 818 871 1805
sales@ixiacom.com

Web site: www.ixiacom.com
General: info@ixiacom.com
Investor Relations: ir@ixiacom.com
Training: training@ixiacom.com
Support: support@ixiacom.com
+1 877 367 4942
+1 818 871 1800 Option 1 (outside USA)
online support form:
http://www.ixiacom.com/support/inquiry/

EMEA
Ixia Technologies Europe Limited
Clarion House, Norreys Drive
Maiden Head SL6 4FL
United Kingdom
+44 1628 408750
FAX +44 1628 639916
VAT No. GB502006125
salesemea@ixiacom.com

Renewals: renewals-emea@ixiacom.com
Support: support-emea@ixiacom.com
+44 1628 408750
online support form:
http://www.ixiacom.com/support/inquiry/?location=emea

Ixia Asia Pacific Headquarters
21 Serangoon North Avenue 5
#04-01
Singapore 5584864
+65.6332.0125
FAX +65.6332.0127
Support-Field-Asia-Pacific@ixiacom.com

Support: Support-Field-Asia-Pacific@ixiacom.com
+1 818 871 1800 (Option 1)
online support form:
http://www.ixiacom.com/support/inquiry/