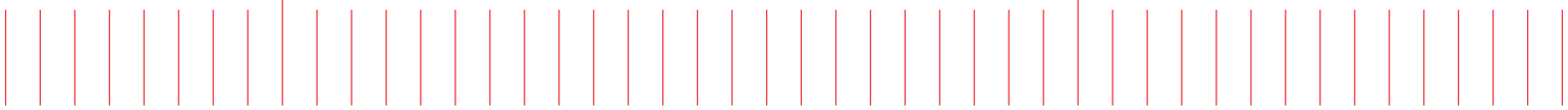
UHD100T32

Release 1.3

User Guide



ixia
A Keysight Business

Document version: 202104161050+05:30

Notices

Copyright Notice

© Keysight Technologies 2020–2021

No part of this document may be reproduced in any form or by any means (including electronic storage and retrieval or translation into a foreign language) without prior agreement and written consent from Keysight Technologies, Inc. as governed by United States and international copyright laws.

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 of 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 shall control.

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.

U.S. Government Rights

The Software is "commercial computer software," as defined by Federal Acquisition Regulation ("FAR") 2.101. Pursuant to FAR 12.212 and 27.405-3 and Department of Defense FAR Supplement ("DFARS") 227.7202, the U.S. government acquires commercial computer software under the same terms by which the software is customarily provided to the public. Accordingly, Keysight provides the Software to U.S. government customers under its standard commercial license, which is embodied in its End User License Agreement (EULA), a copy of which can be found at http://www.keysight.com/find/sweula. The license set forth in the EULA represents the exclusive authority by which the U.S. government may use, modify, distribute, or disclose the Software. The EULA and the license set forth therein, does not require or permit, among other things, that Keysight: (1) Furnish technical information related to commercial computer software or commercial computer software documentation that is not customarily provided to the public; or (2) Relinquish to, or otherwise provide, the government rights in excess of these rights customarily provided to the public to use, modify, reproduce, release, perform, display, or disclose commercial computer software or commercial computer software documentation. No additional government requirements beyond those set forth in the EULA shall apply, except to the extent that those terms, rights, or licenses are explicitly required from all providers of commercial computer software pursuant to the FAR and the DFARS and are set forth specifically in writing elsewhere in the EULA. Keysight shall be under no obligation to update, revise or otherwise modify the Software. With respect to any technical data as defined by FAR 2.101, pursuant to FAR 12.211 and 27.404.2 and DFARS 227.7102, the U.S. government acquires no greater than Limited Rights as defined in FAR 27.401 or DFAR 227.7103-5 (c), as applicable in any technical data. 52.227-14 (June 1987) or DFAR 252.227-7015 (b) (2) (November 1995), as applicable in any technical data.

This page intentionally left blank.

Contacting Us

Keysight headquarters

1400 Fountaingrove Parkway
Santa Rosa, CA 95403-1738
+1 877 367 4942 – Toll-free North America
+1 818 871 1800 – Outside North America
+1.818.871.1805 – Fax
www.ixiacom.com/contact/info

Support

Global Support	+1 818 595 2599	support@ixiacom.com
Regional and local support contacts:		
APAC Support	+91 80 4939 6410	support@ixiacom.com
Australia	+61-742434942	support@ixiacom.com
EMEA Support	+40 21 301 5699	support-emea@ixiacom.com
Greater China Region	+400 898 0598	support-china@ixiacom.com
Hong Kong	+852-30084465	support@ixiacom.com
India Office	+91 80 4939 6410	support-india@ixiacom.com
Japan Head Office	+81 3 5326 1980	support-japan@ixiacom.com
Korea Office	+82 2 3461 0095	support-korea@ixiacom.com
Singapore Office	+65-6215-7700	support@ixiacom.com
Taiwan (local toll-free number)	00801856991	support@ixiacom.com

Documentation conventions

The following documentation conventions are used in this guide:

Describing interactions with the UI

You can interact with products by using different input methods: keyboard, mouse, touch, and more. So in most parts of the user documentation, generic verbs have been used that work with any input method. In cases where input-neutral verbs do not work, mouse-specific verbs are used as the first choice, followed by touch-specific verbs as the second choice.

See the following table for examples on how you can interpret the different input methods.

Input-neutral	Mouse	Touch
Select **Modify**.	Click **Modify**.	Tap **Modify**.
Select **Accounts** > **Other accounts** > **Add an account**.	Click **Accounts** > **Other accounts** > **Add an account**.	Tap **Accounts** > **Other accounts** > **Add an account**.
To open the document in Outline view, select **View** > **Outline**.	To open the document in Outline view, click **View** > **Outline**.	To open the document in Outline view, tap **View** > **Outline**.
Select **Protocols**.	Click the **Protocols** tab.	Tap **Protocols**.
-NA-	Double-click the **Client** wizard.	Double-tap the **Client** wizard.
Open the **Packages** context menu.	Right-click **Packages** to open the shortcut menu.	Long tap **Packages** to open the shortcut menu.

Deprecated words

The following words have been replaced with new words, considering the audience profile, our modern approach to voice and style, and our emphasis to use input-neutral terms that support all input methods.

Old usage...	New usage...
shortcut menu, right-click menu	context menu
click, right-click	select
drag and drop	drag

CONTENTS

Contacting Us ..... **iv**

Documentation conventions ..... **v**

Chapter 1 Overview of UHD **1**

Introduction to UHD 1

Introduction to the UHD web UI 1

Chapter 2 Prerequisites **3**

Chapter 3 UHD Workflow **5**

Chapter 3 What is... ..... **6**

Egress tracking 6

Data capture 6

Priority Flow Control 7

PAUSE Frame Format 7

Chapter 4 How do I... ..... **11**

Sign in to UHD 13

Open a session 13

Edit license settings 13

Define TAP settings 14

Configure a new scenario 15

Start traffic 15

Configure a test scenario by using a config file 16

Clear the current configurations and save a new configuration 16

Select a scenario from the list of sample scenarios 16

Edit a topology 16
Add traffic 16
Edit traffic item and set up flow groups 17
Edit traffic item 17
Set up flow group 17
Start a protocol 17
Perform protocol actions 17
Start egress tracking 18
Capture data packets 19
Turn on PFC 20
Perform traffic actions 22
View statistics 23
View API 23
Test large number of routes 23
Chapter 5 UI **27**
UI: Port status 27
UI: Open Session 28
UI: License settings 28
UI: Overview 29
UI: Traffic 29
UI: Protocol 32
UI: Capture 33
INDEX **35**

CHAPTER 1 Overview of UHD

The UHD100T32 User Guide describes UHD and its usage. It helps you to configure the UHD test equipment with minimal efforts by using the UHD web UI.

Introduction to UHD

UHD100T32 is the industry's first test solution that is purpose-built to address the density challenges of validating 100 GE devices and networks in a more cost-effective way. In just a 1U form-factor, the fixed chassis provides 32 QSFP28 100 GE ports, ready for use cases that range from white box production-line testing to data center pre- and post-deployment testing.

UHD100T32 has fan out modes, which support 100/50/40/25/10 GE speeds. It also includes technology for layer 2 to 3 traffic generation and analysis. Optional routing protocols are available that include OSPF, BGP, ISIS, and RFC 2544 benchmark test capabilities.

Introduction to the UHD web UI

UHD web app is a web-based client UI for layer 2 to 3 traffic generation test application, and is most commonly used to test routing and switching networks.

UHD web app supports multiple concurrent users and sessions, and allows multiple users to access a session, or a user to access multiple sessions simultaneously.

UHD web app has a built-in REST API browser that helps users to configure the test tool through a UI, and then correlate the change directly to REST commands.

This page intentionally left blank.

CHAPTER 2 Prerequisites

Following are the prerequisites to install UHD100T32:

Software requirement

- UHD100T32 1.3

Hardware requirement

- UHD100T32 fixed chassis

Supported browsers

- Google Chrome 75 or later
- Mozilla Firefox 49 or later
- Microsoft Edge 44.17763.1.0 or later

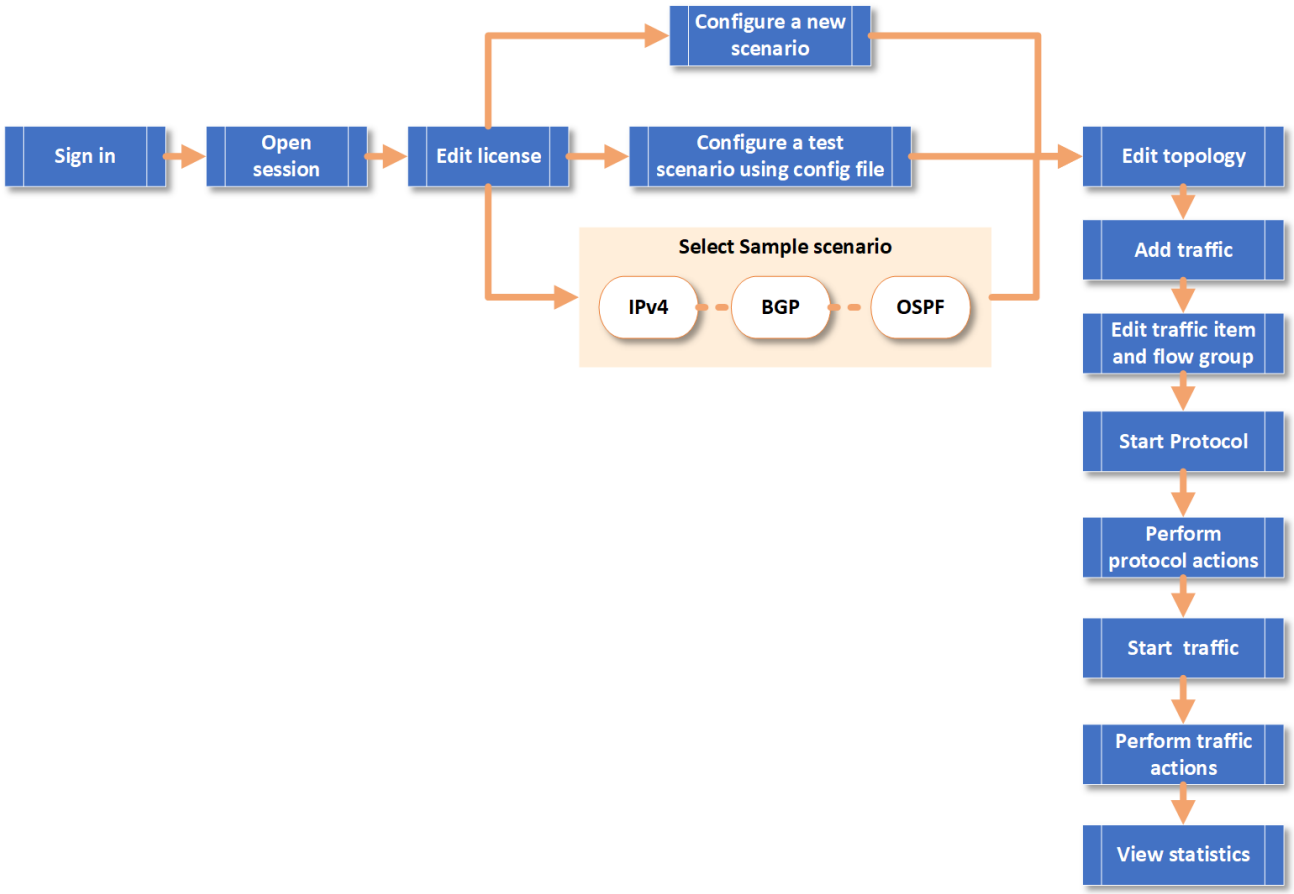
Note: We recommend you to use Adobe Reader for viewing the UHD User Guide.

- Apple Safari 12.1.1 or later

This page intentionally left blank.

CHAPTER 3 UHD Workflow

The following image shows the UHD workflow:



CHAPTER 3 What is...

The 'What is' section contains a list of topics that will help you to understand the concept of certain functionalities of UHD.

Section contents:

Egress tracking **6**

Data capture **6**

Priority Flow Control **7**

PAUSE Frame Format 7

Egress tracking

Egress tracking provides the ability to track statistics on a per-field-value basis for a specific protocol field in the received packets. Up to 10 bits from the protocol field may be used. A different egress tracking field selection may be done on each test port.

UHD supports egress tracking for the following protocol fields:

- Outer VLAN priority – 3 bits
- Outer VLAN ID – least significant 4 bits
- Outer VLAN ID – least significant 10 bits
- Inner VLAN priority – 3 bits
- Inner VLAN ID – least significant 4 bits
- Inner VLAN ID – least significant 10 bits
- VXLAN VNI – least significant 4 bits
- VXLAN VNI – least significant 10 bits
- IPv4 TOS precedence – 3 bits
- IPv4 DSCP – 6 bits
- IPv6 DSCP – most significant 6 bits of the traffic class field
- IPv6 ECN – least significant 2 bits of the traffic class field

Note: The least significant bit of the field is the rightmost bit.

Data capture

With UHD you can capture up to 1 MB of data packets. By default, UHD captures all received packets. You can use capture filters to capture specific packets. This capture allows some space for per-packet overhead. You can capture received packets only, and you can capture on one port per resource group.

Following are the filter conditions for the capture:

- IPv4 length
- IPv4 source address
- IPv4 destination address

See UI: Capture for more information. See Capture data packets to know the data capture procedure.

Priority Flow Control

Priority flow control (PFC), as defined in IEEE 802.1Qbb, operates within a full-duplex point-to-point link between two MACs to prevent the dropping of frames due to congestion. It is an extension to the standard PAUSE-based flow control defined in IEEE 802.3x. When congestion is detected on a MAC, it sends PAUSE frames to its peer to enable flow control. When a PAUSE frame is received, a MAC stops sending traffic until the timeout specified in the PAUSE frame has expired, or when another PAUSE frame that indicates that flow control should be disabled is received. Standard flow control stops all traffic on the MAC whereas PFC stops only traffic with a specific priority.

UHD can test a DUT's handling of PFC by acting as both the source and destination of high-rate traffic sent on priority A and other priorities, going through the DUT. At the same time, the UHD Rx port sends a storm of PFC PAUSE frames to enable flow control on priority A. Upon receipt of the PAUSE frames, the DUT should stop forwarding the packets with priority A to the UHD Rx port but keep sending packets on the other priorities. The DUT may also send corresponding PFC PAUSE frames to the UHD Tx port to stop the traffic and prevent its buffers from overflowing. Upon receiving the PAUSE frames, the UHD Tx port must stop transmitting priority A packets.

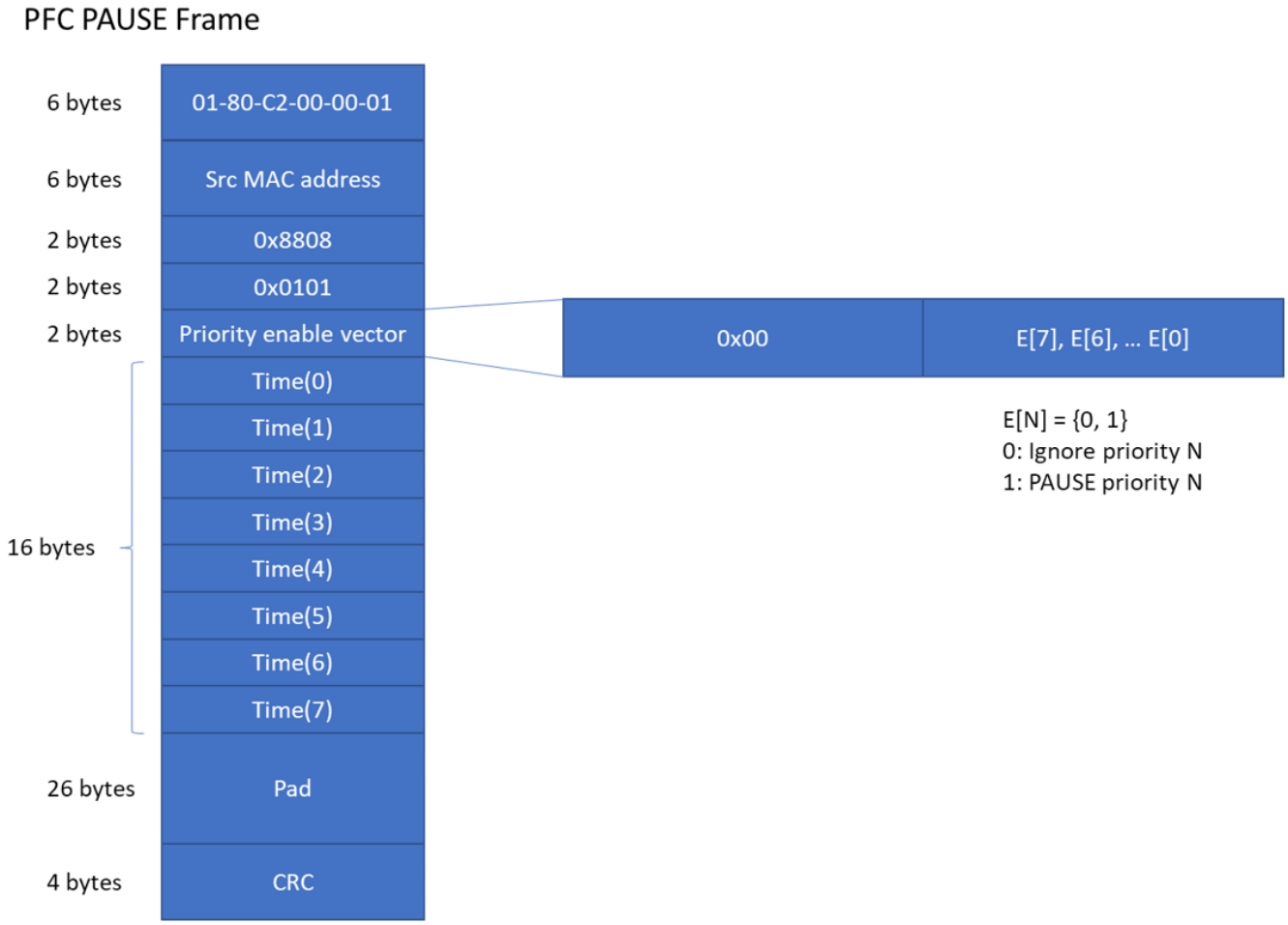
The same test can also be used to verify standard flow control, with the difference being that a priority does not need to be specified in either the traffic or the PAUSE frames. In this case, upon receiving the PAUSE frames, the DUT should stop sending any traffic to the UHD Rx port.

PAUSE Frame Format

The PAUSE frame is a type of MAC Control frame. The MAC Control header immediately follows the Ethernet header, and uses an ethertype of 0x8808. The MAC Control header starts with a 2-byte MAC Control opcode, and then the contents of the subsequent bytes is determined by each specific opcode. The PFC PAUSE frame has an opcode of 0x0101, and the standard PAUSE frame has an opcode of 0x0001. Also, all PAUSE frames are sent using the multicast destination address of 01-80-C2-00-00-01.

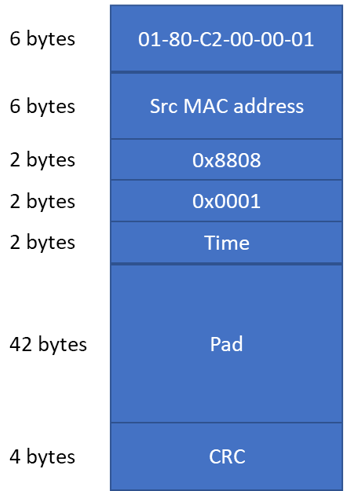
After the opcode, the PFC PAUSE frame contains a 2-byte priority enable vector, and then eight 2-byte time quanta values – one for each priority. The most significant byte of the priority enable vector is reserved, while the least significant byte indicates whether flow control is enabled for each priority

(leftmost bit is for priority 7 and rightmost bit is for priority 0). The time quanta value is the requested duration of the pause and is measured in units equal to 512 bit times (one bit time is the time it takes for one bit to be sent at the current line speed).



For the standard PAUSE frame, the opcode is 0x0001, which followed by a 2-byte time quanta field.

Standard (802.3x) PAUSE Frame



Key points

Unless stated otherwise, all port-based requirements apply to ports on all test speeds, which includes fan-out ports.

- Flow control can be enabled on a per-port basis.
- Each port can have either PFC or standard flow control enabled, but not both at the same time.
- Each port will support 8 priorities.
- Each port will support 8 PFC queues.
- Each PFC queue can be assigned only 1 priority, though different PFC queues can have the same priority.
- If PFC is enabled on a port, any traffic item using the port as source can be assigned to a PFC queue.
- If PFC is enabled on a port, and a PFC PAUSE frame is received with at least one priority enabled in its priority enable vector with a non-zero time quanta, any traffic items assigned to a PFC queue with an enabled priority using that port as source will stop sending traffic from that port.
- If traffic was stopped due to the receipt of a PFC PAUSE frame, traffic will resume if a subsequent PAUSE frame is received with traffic's priority set to disabled and/or the corresponding time quanta is zero, and if the traffic is still running on the port.
- If standard flow control is enabled on a port, and a standard PAUSE frame is received with a non-zero time quanta, any traffic items using that port as source will stop sending traffic from that port.
- If traffic was stopped due to the receipt of a standard PAUSE frame, traffic will resume if a subsequent PAUSE frame is received with the time quanta set to zero, and if the traffic is still running on the port.
- A standard or PFC PAUSE frame can be created using a "Raw" traffic item.

Not Supported

- The sending of any PAUSE frames outside of the context of a "Raw" traffic item will not be supported (i.e. UHD will not send PAUSE frames due to perceived congestion to support lossless traffic).
- The changing of the directed address from the default of "01 80 C2 00 00 01" is not supported.
- PFC delay and the specification of the delay quanta and/or delay time is not supported.
- Per-stream receive statistics (traffic item rx stats and flow rx stats) for PAUSE frame traffic is not supported.

CHAPTER 4 How do I...

The 'How do I' section contains a list of topics that will help you to configure UHD by using the UHD web UI.

Section contents:

Sign in to UHD **13**

Open a session **13**

Edit license settings **13**

Define TAP settings **14**

Configure a new scenario **15**

Start traffic 15

Configure a test scenario by using a config file **16**

Clear the current configurations and save a new configuration 16

Select a scenario from the list of sample scenarios **16**

Edit a topology **16**

Add traffic **16**

Edit traffic item and set up flow groups **17**

Edit traffic item 17

Set up flow group 17

Start a protocol **17**

Perform protocol actions **17**

Start egress tracking **18**

Capture data packets **19**

Turn on PFC **20**

Perform traffic actions **22**

View statistics **23**

View API **23**

Test large number of routes **23**

Sign in to UHD

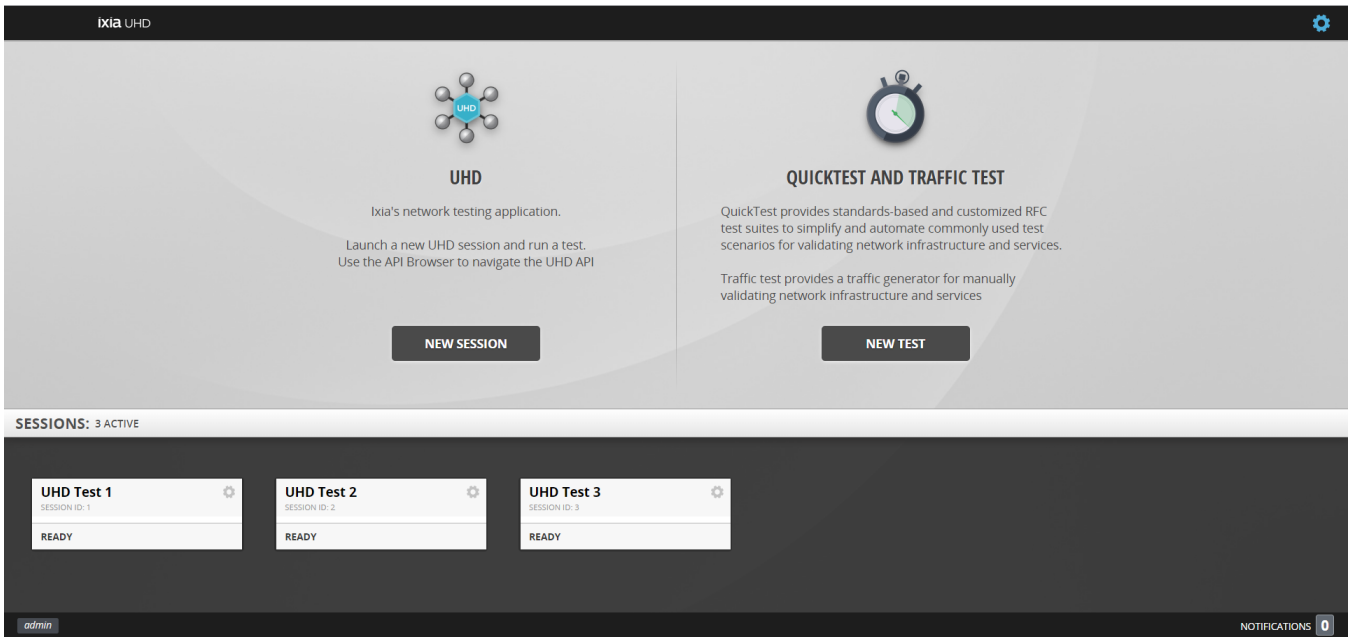
To sign in to the UHD fixed chassis, do the following:

1. Provide the IP address of the UHD fixed chassis in the URL.
2. Enter your credentials and select **LOGIN**.

Open a session

The web UI allows you to create new sessions and work with multiple sessions. You can also work with the existing sessions.

- To create a new session, in the UHD section, select **NEW SESSION**.
- To open an existing session, select a session from the saved sessions in the **SESSIONS** section.



Edit license settings

To edit a license, do the following:

1. Select from the top right corner and select **SETTINGS**.
2. In the **License** section, edit the license settings as follows:
   a. Select a value for **Licensing Mode**. **Mixed** is the default licensing mode.
   b. In the **License Servers** box, keep the default value, which is `localuhd`.
   c. Select a value from the **Tier Level** list.

Note: For Perpetual licenses, you can keep the default license settings. For Subscription licenses, select the correct tier from the **Tier Level** dropdown.

UHD automatically saves the changes.

Define TAP settings

This section describes the major tasks required to define layer 1 QSFP28 TAP settings for UHD.

To define the TAP settings, do the following:

1. Sign in to the admin shell.
2. Use the `uhd_tapct` to define layer 1 QSFP28 TAP settings for UHD.
   Usage: `uhd_l1tap [command] [args]`
   Available commands:
   - `set <port # between 1-32> <tx-pre-tap> <tx-main-tap> <tx-post-tap>`
   - `get <port # between 1-32>`

   Examples:
   - `uhd_tapctl set 1 6 0 0`
   - `uhd_tapctl get 1`

   Example output:

```
$ uhd_tapctl get 1
Port, Lane, TxPre, TxMain, TxPost
1,0,4,0,0,
1,1,4,0,0,
1,2,4,0,0,
```

1,3,4,0,0,

```
kcos-framework-shell-85b5d56959-bqmk8:~$ uhd_tapctl

uhd_tapctl is beta utility to set/get layer 1 QSFP28 tap settings for UHD
Usage: uhd_l1tap [command] [args]

Commands:

        set <port # between 1-32> <tx-pre-tap> <tx-main-tap> <tx-post-tap>
        get <port # between 1-32>

Examples:

        uhd_tapctl set 1 6 0 0
        uhd_tapctl get 1
kcos-framework-shell-85b5d56959-bqmk8:~$ uhd_tapctl get 1
Port, Lane, TxPre, TxMain, TxPost
1,0,4,0,0,
1,1,4,0,0,
1,2,4,0,0,
1,3,4,0,0,
kcos-framework-shell-85b5d56959-bqmk8:~$ uhd_tapctl set 1 6 0 0
kcos-framework-shell-85b5d56959-bqmk8:~$ uhd_tapctl get 1
Port, Lane, TxPre, TxMain, TxPost
1,0,6,0,0,
1,1,6,0,0,
1,2,6,0,0,
1,3,6,0,0,
kcos-framework-shell-85b5d56959-bqmk8:~$
```

Configure a new scenario

To configure a new scenario, do the following:

1. On the **Overview** page, select **Add Protocol**.
2. In the **Select Protocols** pane, select the protocols from the list of supported protocols, for example, IPv4.
3. After you select a protocol, the **Ports** and **LAGs** pane appears.
   a. To add ports, select the available ports under the chassis and select **New Topology**. To understand the status of ports, see Port status .
   b. To add LAG, select **LAGs** and then select the **Add LAG**.
   Select the available ports under the chassis and then select **Done Selecting Ports**, or select **New Topology**.
   To configure LAG or LACP protocol setting, select **L1/LAG Settings** in the LAG/Port selection dialog box or select **L1** in scenario editor port icon.
4. UHD creates a new topology for you. Configure the topology according to your requirements.

Start traffic

To start traffic, on the **Traffic** page, select **Traffic** to start traffic.

Configure a test scenario by using a config file

You can configure test scenarios by uploading the ixncfg or json configuration files. To upload a configuration file, do the following:

1. Select **Overview**.
2. Select **Files**, and then select **Browse to upload a file** to upload an ixncfg config file, for example, ISIS_L3.ixncfg.
3. After you upload the file, you can edit the topology according to your needs and you can start the test.

Clear the current configurations and save a new configuration

To clear the current configurations and to save a new configuration, do the following:

1. Select **Files**, and then select **New** to clear the current configuration.
2. Select **Save As** to save a new configuration.

Select a scenario from the list of sample scenarios

You can choose the test scenarios from the sample scenarios or recently used scenarios. To open a sample scenario, do the following:

1. In the **Samples** section, select a sample scenario that you want to test. The test topology for the selected scenario appears.
2. Configure the topology according to your needs.

Note: Currently, the sample scenarios of IPv4, BGPv4, ISIS, and OSPFv2 are available in UHD.

Edit a topology

After you create or select a scenario, UHD shows an interactive topology that you can edit.

To edit the topology, do the following:

1. Select the different parts of the interactive topology to view the respective settings in the bottom pane.
2. Edit the columns with the icon.
3. Type your value and select **Enter**. UHD automatically saves you changes.

Add traffic

You can configure the traffic streams on the ports. To add a traffic stream, do the following:

1. Select the **Traffic** page.
2. Select **Add**, and then select **Add Traffic Item** to open the **Add Traffic** pane.

3. Select the traffic type from the list.
4. Select the source and destination ports from the **Sources** and **Destinations** sections respectively.
5. Select **New Traffic Item**.

Note: Changing mesh settings is optional.

Edit traffic item and set up flow groups

The **Traffic Item** grid and the **Flow Groups** grid are interactive. You can edit the fields in the grid and save the configuration.

Note: Editing the traffic item and setting up the flow groups is optional.

Edit traffic item

To edit a traffic item, do the following:

1. Select **Traffic Item** to view flow groups grid.
2. Select the **Frame Size** column, edit the value in **Frame Size**, and then select **OK**.

Set up flow group

To set up flow groups, create the flow groups based on the selectable packet fields. One flow group per high-level stream is created for each selected field.

Start a protocol

You can start a protocol by using any one of the following methods on the **Protocol** page:

- Select **Test**, and then select **Start**. This initiates the complete test scenario, which includes connecting to ports, starting protocols, and starting traffic.
- Select **Protocol** to start all the protocols configured in the test session.

Perform protocol actions

To perform the various protocol actions, do the following:

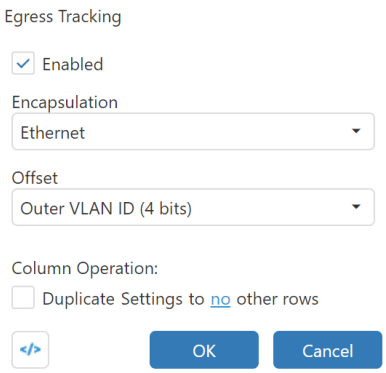
1. On the **Protocols** page, select **Actions** to open the **Protocol Actions** pane.
2. Select a protocol from the **Protocols** list and select the action that you want to perform on the selected protocol from the **GLOBAL ACTIONS** list and the **SELECTED ITEMS** list.
    - From the **GLOBAL ACTIONS** list, do the following:
        - Select **Connect Ports** to connect to the topology.
        - Select **Ports** to view the **Port Picker** window to edit the port selection.
        - Select **Apply Changes** to apply the changes.

- From the **SELECTED ITEMS** list, do the following:
  - Select **Start Selected** to start the selected protocol.
  - Select **Stop Selected** to stop the selected protocol.
  - Select **Abort Selected** to remove the configured plug-ins from the port CPU to return the protocols to the unconfigured state.
  - Select **Restart Down Sessions** to restart the failed sessions to generate the flows on the selected traffic item.

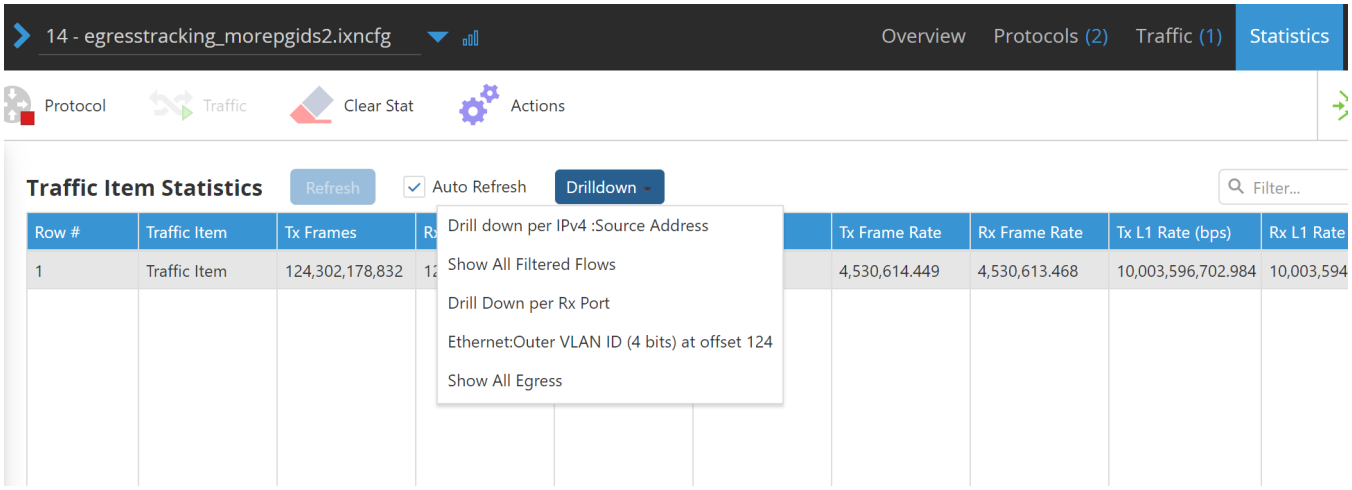
Start egress tracking

To start egress tracking of a traffic item, do the following:

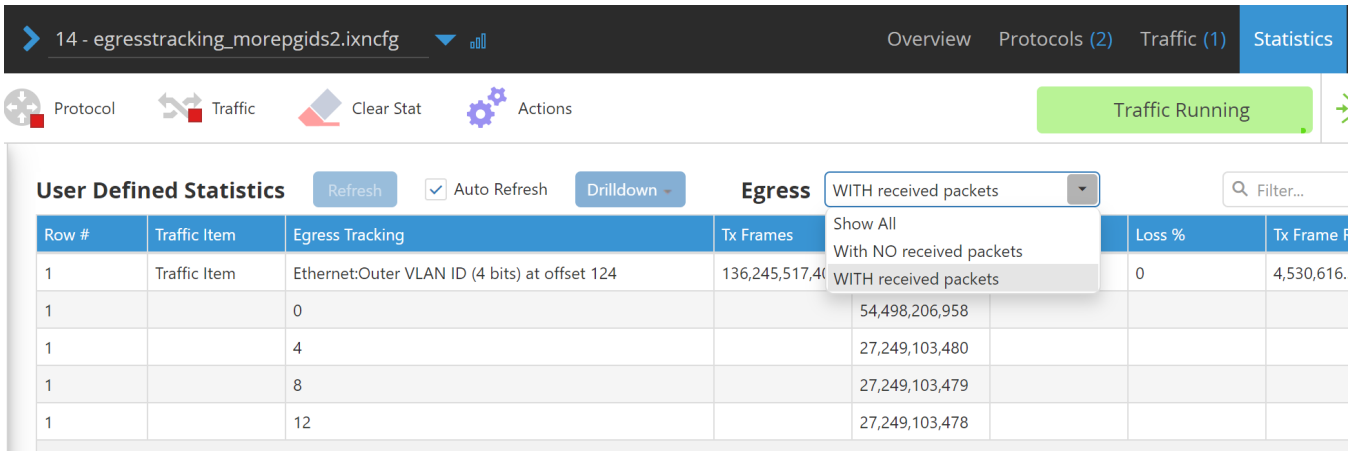
1. Select to open the **Grid View Configurations** box and select **Egress Tracking** to add **Egress Tracking** column to the grid.
2. Select a traffic item and edit the value in the **Egress Tracking** column for the traffic item to turn on egress tracking and select the protocol field.



3. After turning on the egress tracking, regenerate and apply the traffic item, and then start traffic.
4. After traffic is running, go to the **Statistics** view and select **Traffic Item Statistics**.
5. On the **Traffic Item Statistics** grid, select the traffic item from the grid and select the egress tracking field in the **Drilldown** drop-down list to show the egress tracking statistics view. By default, only values present in the protocol field of the received packets are displayed.



6. Select the view you want from the **Egress** drop-down list. Following are the available views:
   - **Show All** - view the rows of rows for all possible values.
   - **With NO received packets** - view the rows for only those values with no received packets.
   - **With received packets** - view the rows for only those values with received packets.



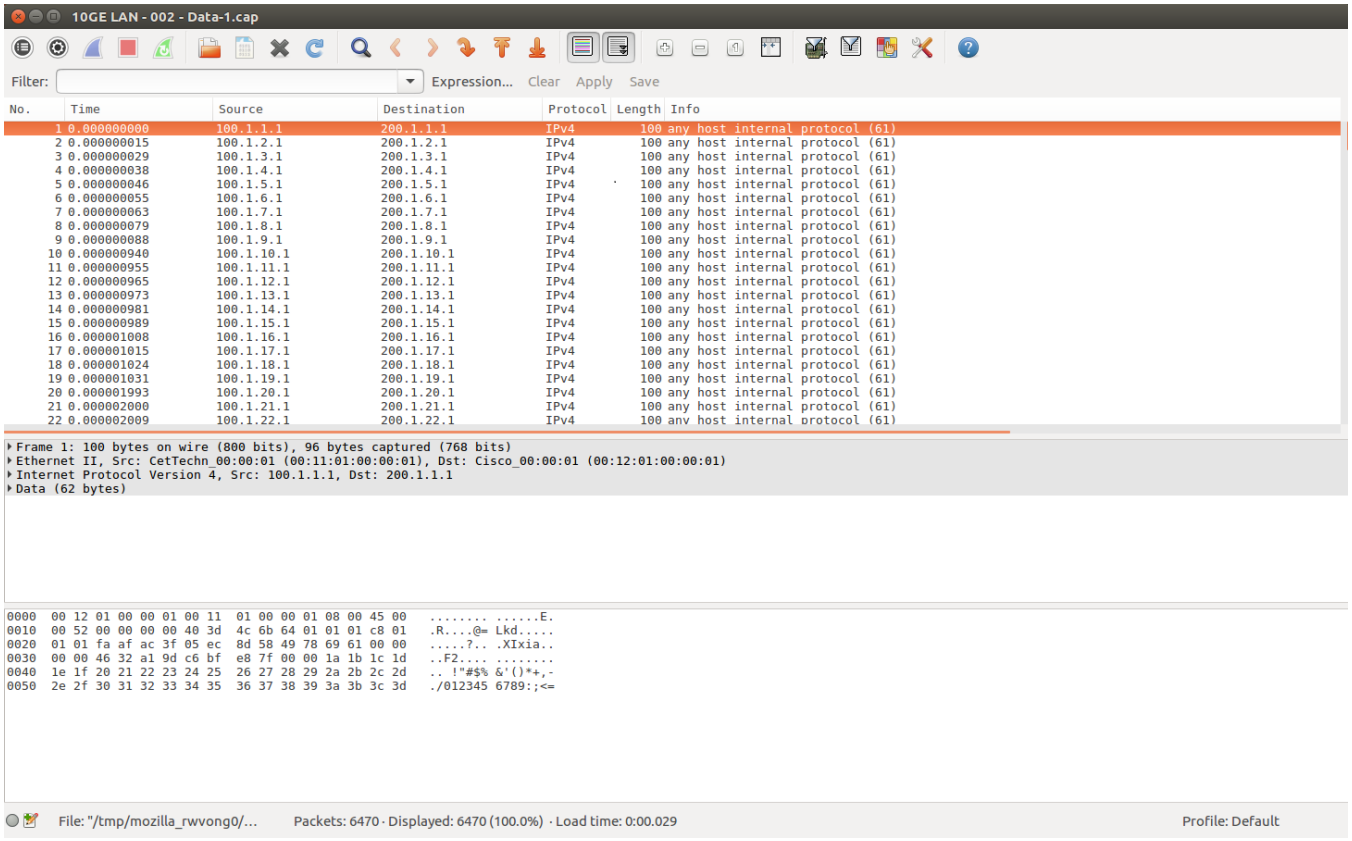
Note: If the protocol header containing the selected egress tracking field is not present in a received packet, that packet is counted as Invalid encapsulation. This value is the largest possible value for the selected field based on its field bit width.

Capture data packets

To capture data packets, do the following:

1. Select the **Capture** icon to open up the **Capture Settings** view.
2. Select the port where you want to capture packets, and then select the **Enable Data Capture** checkbox.

3. Select **Actions**, and then select **Start All Capture**. In the **All Ports** table, the port icon changes to show that capture is running.
4. When the data has been captured, or when you select the **Stop All Capture** action, IxNetwork stops capture and retrieves the captured packets. This takes a few seconds. The port icon changes again to show that capture is not running. A list of packet captures appears at the bottom right corner, starting with the most recent capture. You can then select the download icon to display the captured packets in Wireshark.



When filtering by IPv4 address, you specify a value and a mask, with each 1 bit in the mask indicating it's significant.

For example, if you want to capture packets with an address of 100.1.1.1, use address 100.1.1.1 and mask 255.255.255.255.

If you want to capture packets with any address 100.1.1.x (100.1.1.1, 100.1.1.2, 100.1.1.3, etc.), specify address 100.1.1.1 (the last byte doesn’t matter) and mask 255.255.255.0.

When you have multiple filter conditions, they are ANDed. In other words, each packet must match all filter conditions to be captured.

Turn on PFC

To turn on PFC, complete the following steps:

1. Add two UHD test ports.
2. Select the port to edit the settings.
3. Select **Enable Flow Control** check box and from the Flow Control type list, select either **IEEE 802.1 Qbb** for PFC or **IEEE 802.3x** for standard flow control.
4. If you select PFC flow control, select one or more PFC queues from **PFC & Priority Group** and assign a priority to it.
5. Optional. Add an IPv4 or IPv6 topology on each test port, and configure MAC addresses, VLAN IDs, IP addresses as necessary.
6. Start protocols and wait for IP addresses to be resolved.
7. Add traffic item 1, which needs to be flow controlled. Select here to know the steps.
   a. Set the desired traffic item type.
   b. Select the port 1 (or topology 1) as the source and port 2 (or topology 2) as the destination.
   c. Set the packet header and contents, and frame size to the desired configuration.
   d. Set the rate to continuous at a high rate (close to or at 100% line rate if no background traffic).
   e. Select the entire traffic item for flow tracking.
   f. If you are testing PFC, select the **Stack** column to go to the Packet Editor, then select **Ethernet II** to view the **PFC Queue** field and assign the traffic item 1 to the PFC queue.
8. Add traffic item 2 (PAUSE storm). Select here to know the steps.
   a. Select **Raw** from the traffic item list.
   b. Select port 2 (or topology 2) as the source and port 1 (or topology 1) as the destination and complete one of the following steps:
      - If you are testing PFC:
        i. Change the packet header to **PFC PAUSE** by adding the **PFC PAUSE** header immediately after the **Ethernet II** header, and then remove the original **Ethernet II** header because the **PFC PAUSE** header already has an Ethernet header encapsulated inside.
        ii. Set the priority enable vector to enable the priority of the PFC queue selected in 5d).
        iii. Set the time value for the selected PFC queue/priority to >0.
      - If you are testing standard flow control:
        i. Change the packet header to 802.3x PAUSE.
        ii. Set the pause time to >0.
   c. Set the packet size to fixed 64 bytes.
   d. Set the source and destination addresses.
   e. Set the rate to a desired value, with a non-continuous (fixed duration or fixed packet count) transmission mode and a small start delay.

9. (Optional) Add one or more background traffic items. For each traffic item, do the steps here.
    a. Set the desired traffic item type.
    b. Select the port 1 (or topology 1) as the source and port 2 (or topology 2) as the destination.
    c. Set the packet header and contents, and frame size to the desired configuration.
    d. Set the rate to continuous with a value such that the sum of the rate of traffic item 1 plus that of all background traffic items is close to or at 100% line rate.
    e. Select the entire traffic item for flow tracking.
    f. If doing PFC testing, assign the traffic items to one of the PFC queues enabled in step 3) that is not the same as the one used by traffic item 1.
10. Apply and start traffic.
11. View the traffic item statistics. Select here to know the steps.
    a. Traffic item 1 and all background traffic items should be sending and receiving at the configured rate.
    b. After the delay configured in 6g), the PAUSE frames are sent, and the receive rate of traffic item 1 should go to 0. Eventually, the transmit rate of traffic item 1 should go to 0 as well.
    c. After traffic item 2 is not longer sending packets (transmit rate for port 2 is 0), the transmit and receive rate for traffic item 1 should go back to the configured rate.

Perform traffic actions

To perform the various traffic actions, do the following:

1. On the **Protocols** page, select **Actions** to open the **Traffic Actions** pane.
2. Select a traffic item from the **Traffic Items** list and select the action that you want to perform from the **Traffic Actions** pane.

- From the **ALL ITEMS** list, do the following:
    - Select **Delete All** to delete all the traffic items.
    - Select **Generate All** to generate the flows of all the traffic items that you created.
    - Select **Start All** to start traffic for all the traffic items.
    - Select **Stop All** to stop traffic for all the traffic items.
- From the **TRAFFIC ITEM** list, do the following:
    - Select **Delete Traffic Item** to delete the selected traffic item.
    - Select **Generate Traffic Item** to generate the flows of the selected traffic item.
    - Select **Start** to start the selected traffic item.
    - Select **Stop** to stop the selected traffic item.
    - Select **Pause** to pause traffic on the selected traffic item.
    - Select **Duplicate Traffic Item** to create a duplicate copy of the item.

- Select **Convert To Raw** to create a duplicate of the selected traffic item to send traffic on a port-to-port basis, without the use of protocol interfaces.

View statistics

You can view the traffic statistics from the **Statistics** page. You can also view the different statistics such as port statistics, traffic flow statistics, and layer 2 to 3 traffic test summary statistics.

To view the port statistics, do the following:

1. Select **Statistics**.
2. In the left pane, under **Ports**, select **Port Statistics**. The port statistics appears.

To view layer 2 to 3 traffic test summary statistics, do the following:

1. Select **Statistics**.
2. In the left pane, under **Traffics**, select **L2-L3 Test Summary Statistics**. The layer 2 to 3 test summary statistics appears.

To view flow statistics, do the following:

1. Select **Statistics**.
2. In the left pane, under **Traffics**, select **Flow Statistics**. The flow statistics appears.

View API

You can view the UHD APIs in the UHD API browser. The API data is available in a hierarchical format in this browser. You can access each level of the hierarchy with a view of peers, attributes, executables, errors, and child levels.

To open the API browser, select on the top menu.

Test large number of routes

With the Perpetual or Tier3 (U100-PREMIUM) license, UHD100T32 supports a special hardware mode which can test a very large number of IPv4 and IPv6 routes using 32-bit counters, but with limited realism, based on the following conditions:

- All routes must be a uniform range across the entire test.
- IPv6 routes are restricted to varying in bits 33 to 64, or in bits 97 to 128: 0:0:0:0:ff:ff:ff:ff:0:0:0:0:ff:ff:ff:ff.
- All packets sent from the same port use the same source and destination MAC addresses.
- Only the 100G speed mode is supported.

The following are the only fields that can vary:

- VLAN ID
- IPv4 or IPv6 source address (32 bits)
- IPv4 or IPv6 destination address (32 bits)

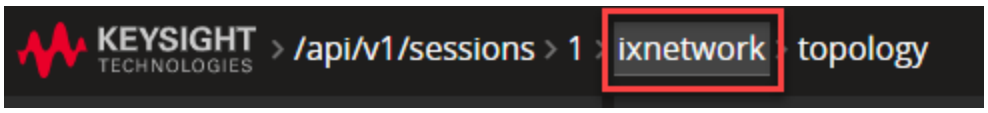
The default hardware mode is much more flexible, allowing arbitrary source and destination addresses, but only tests up to 1024 routes.

To switch from the default mode to the special hardware mode in the web application, do the following:

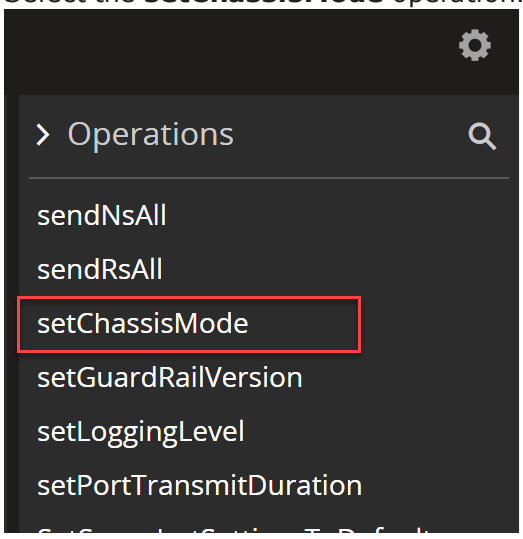
1. Open the API browser by selecting on the top menu.

   Note: To switch to the special hardware mode, you need to ensure that none of the UHD100T32 ports are being used by anyone.

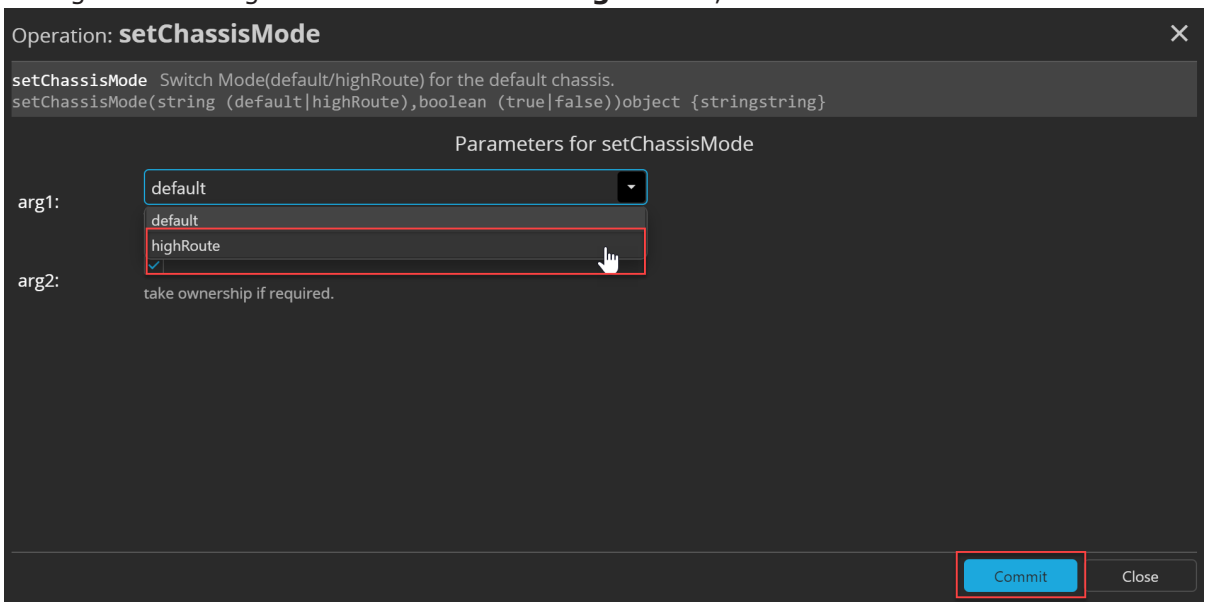
2. Select the **ixnetwork** node.



3. Select the **setChassisMode** operation.



4. Change the first argument from **default** to **highRoute**, and then select **Commit**.



5. It takes about three minutes for the mode change to finish. After it is done, a message showing SUCCESS appears.
   Select the arrow to the right to check for any issues.

The following is an example of a typical test.

- Configure 32 IPv4 addresses per port, matching the IPv4 addresses on the DUT side.
- Configure a BGP peer on each IPv4 interface, matching the DUT configuration.
- Behind the BGP peers, configure a network group with IPv4 routes. Configure the routes to be uniformly incrementing across all peers and all ports.
- Add a traffic item, setting the **Route Mesh** option to **One - One**.
  If you set the **Src/Dst Mesh** option to **Fully Meshed** (which means sending from every port to every other port), make sure to enable **Allow self-destined**, so that the traffic sent from each port will include the entire range of routes instead of skipping its own routes.

Once you have completed your high route scale tests, use **setChassisMode** again to switch the hardware mode back to the default.

This page intentionally left blank.

CHAPTER 5 UI

The 'UI' section contains a list of topics describing the UI labels of UHD web UI.

Section contents:

UI: Port status **27**

UI: Open Session **28**

UI: License settings **28**

UI: Overview **29**

UI: Traffic **29**

UI: Protocol **32**

UI: Capture **33**

UI: Port status

The following table shows the different statuses of the ports:

Port	Status
	Port is available.
	Port is down.
	Port is unavailable.
	Port is assigned to a topology in the configuration file.

	Port is assigned to the selected topology.
	Another user has reserved this port.

UI: Open Session

The following table shows the names and descriptions of the UI labels on Open Session page:

UI	Description
NEW SESSION	Select to create a new session in the UHD section.
SESSIONS	Select to open an existing session from the list of the saved sessions.

UI: License settings

The following table shows the names and descriptions of the UI labels on License setting page:

UI	Description
Version	Version of Web UI and UHD.
Preferences	Select **Port Ownership** to automatically clear ownership when starting protocol.
License	Select the details of the license: • Licensing Mode: Select the license mode. Available modes are: ▪ Mixed ▪ Perpetual ▪ Subscription **Note:** **Mixed** is the default licensing mode. • License Servers: The name of the license server. Keep default to `localuhd`. • Tier Level: Select the tier level. Available levels are: ▪ Tier 1 ▪ Tier 2 ▪ Tier 3 **Note:** For Perpetual licenses, you can keep the default license settings. For Subscription licenses, select the correct tier from the **Tier Level** dropdown.

Diagnostic	• Select **Current Instance** to run diagnostics. • Select **Past Instances** to view historical diagnostic data.

UI: Overview

The following table shows the names and descriptions of the UI labels on Overview page:

UI	Description
Files	Create, open, save, or delete a configuration file.
Test	Start or stop a test.
Add	Select to add topology, device group, chained device group, stack, protocol, and network group.
Protocol	Run protocol.
Delete	Delete the selected item.

Actions	Protocol actions. Following are the available actions:
	• Global Actions:
	  ▪ Connect Ports: Select to connect ports.
	  ▪ Release Ports: Select to release the connected ports.
	  ▪ Apply Changes: Select to apply the changes.
	• Selected Item
	  ▪ Start Selected: Start selected protocol session.
	  ▪ Stop Selected: Stop selected protocol session.
	  ▪ Abort Selected: Immediately stops all network stack processes for the selected protocol.
	  ▪ Restart Down Sessions: Restarts failed protocol sessions.
	  ▪ Abort: Immediately stops all network stack processes for the selected element in the navigation tree, without attempting to terminate the sessions with the DUT. It also removes the configured plug-ins from the port CPU, returning the protocols to the unconfigured state.
	• Device Group
	  ▪ Start
	  ▪ Stop
	  ▪ Abort

UI: Traffic

The following table shows the names and descriptions of the UI labels on Traffic page:

UI	Description
Files	Create, open, save, or delete a configuration file.
Test	Start or stop a test.
Add	Select to add topology, device group, chained device group, stack, protocol, and network group.
Traffic	Run traffic.
Delete	Delete the selected item.

Actions	Traffic actions. Following are the available actions:
	• All Item:
	  ▪ Delete All: Delete all traffic items.
	  ▪ Generate All: Generate traffic for all traffic items.
	  ▪ Apply All: .
	  ▪ Start All: Start all traffic items.
	  ▪ Stop All: Stop all traffic items.
	• Selected Item
	  ▪ Delete Traffic Item: Delete the selected traffic item.
	  ▪ Generate Traffic Item: Generate traffic for the selected traffic item.
	  ▪ Duplicate Traffic Item: Create a copy of the selected traffic item.
	  ▪ Convert to Raw: Create a new raw version of the selected traffic item, which will have all of the encapsulation and payload information of the original now-raw version.
	• Selected Flow Group
	  ▪ Start: Start traffic for the selected flow group.
	  ▪ Stop: Stop traffic for the selected flow group.
	  ▪ Pause: Pause traffic for the selected flow group.

Traffic Items	This section shows information for all traffic items.
Traffic Item	The name of the traffic item.
State	The current transmit state of the traffic item, options include the following: • Start: If this button is green you can select it to start transmitting traffic on this traffic item. • Pause: If this button is blue you can select it to pause traffic on this traffic item. • Stop: If this button is red you can select it to stop traffic on this traffic item.

Enabled	Activate the selected traffic item. The default is turned on.
Scr/Dest Mesh	The traffic flow meshing type between the different source endpoint and destination endpoint pairs, which can be as follows: • One-One • Many to Many • Fully Meshed
Route Mesh	The traffic flow type between each pair of source route endpoint and destination route endpoint, which can be as follows: • One-One • Fully Meshed
Bi-Directional	Allow traffic to be sent in forward and reverse destination.
Statistics Tracking	Select tracking filters for generating statistics.
Destination	Destination of the traffic.
Sources	Source of the traffic.
Stack	Stack used for generating traffic.
Frame Size	The packet size for this endpoint set.
Frame rate	The packet rate for this endpoint set.
Egress Tracking	Turn on egress tracking for the selected traffic item, based on encapsulation and offset.
Payload	The payload pattern of the configured encapsulation set.
Flow Groups	This section shows information for all flow groups.
State	The state of the flow group's transmit port.
Enabled	If selected, the corresponding flow group is turned on. When not selected, the flow groups do not get applied to the transmit ports. Only enabled flow groups can be started. They can be enabled only when traffic is stopped.
Tx Port	The name of the transmit port.
Rx Port	The name of the receiving ports.
Flow Name	The name of the flow group.
Stack	Stack used by this flow group.

Packets	Select to preview the packets.
Frame Size	The frame size used by this flow group.
Frame Rate	The frame rate used by this flow group.
Frame Payload	The type of frame payload used by this flow group.
Applied Frame Size	This field cannot be edited.
CRC	The type of CRC error used by this flow group.
Preamble Size	The preamble size used by this flow group.
Transmission	The transmission mode used by this flow group.
Dest MAC Address	The destination MAC address for this flow group.
Src MAC Address	The source MAC address for this flow group.

UI: Protocol

The following table shows the names and descriptions of the UI labels on Protocol page:

UI	Description
Topology	Name of the topology used in this protocol.
Ports	Ports used in the topology.
Device Group	The identifier of the device group in the topology.
Multiplier	Ratio of protocol elements, or protocol instances, that are created when a stack is instantiated.
Count	Count of devices.
Stack	Name of the stack.
Enable GRATARP or RARP	Select this check box to activate the Send GRATARP or RARP function, where you can choose to send either GRATARP or RARP packets during the IPv4/Ethernet stack startup.
Send GRATARP or RARP	Select from the following options to send the packet when the IPv4/Ethernet stack starts: • Send GRATARP

	• Send RARP

UI: Capture

The following table shows the names and descriptions of the UI labels on Capture page:

UI	Description
Enable Control Capture	Capture control-plane (protocol) packets on the selected port.
Enable Data Capture	Capture data-plane packets on the selected port, not including protocol packets.
Actions	Start All Capture: Start capture on all ports. Stop All Capture: Stop capture on all ports. Delete All Capture: Delete all captured files on the selected port.
IPv4 length	Filter on the IPv4 length field in an IPv4 packet. You specify the range of length values that you're interested in. The default range is 46 bytes (corresponding to a 64-byte Ethernet frame) to 9198 bytes.
IPv4 source address	Filter based on the IPv4 source address in an IPv4 packet.
IPv4 destination address	Filter based on the IPv4 destination address in an IPv4 packet.
Captured Files	List of packet captures. Most recent capture being on top.

This page intentionally left blank.

INDEX

A

adding traffic 16

adding traffic streams 16

C

changing topologies 16

choosing scenarios 16

choosing test scenarios 16

clearing current configurations 16

clearing existing configurations 16

configuring new scenarios 15

configuring test scenarios 16

configuring traffic items 17

configuring traffic streams 16

creating new sessions 13

customer assistance iv

D

defining tap settings 14

deprecated words v

documentation conventions v

E

editing license settings 13

editing licenses 13

editing topologies 16

editing traffic items 17

H

hardware prerequisites 3

hardware requirements 3

how do I 11

how to 11

I

initiating protocols 17

initiating traffic 15

introduction to UHD web UI 1

introduction to UHD100T32 1

K

keyboard interactions v

L

logging on 13

M

modifying license settings 13

modifying licenses 13

modifying topologies 16

modifying traffic items 17

mouse interactions v

O

opening sessions 13

overview of UHD web UI 1

overview of UHD100T32 1

P

performing protocol actions 17

performing traffic actions 22

port statuses 27

prerequisites 3

product support iv

R

requirements 3

running protocols 17

S

saving new configurations 16

selecting scenarios 16

selecting test scenarios 16

setting up flow groups 17

setting up traffic items 17

signing in 13

software prerequisites 3

software requirements 3

starting protocols 17

starting traffic 15

status of the ports 27

support services iv

supported browsers 3

T

technical support iv

test high route scale 23

test large number of routes 23

touch interactions v

U

UHD process 5

UHD web UI introduction 1

UHD web UI overview 1

UHD workflow 5

UHD100T32 introduction 1

UHD100T32 overview 1

V

viewing APIs 23

viewing flow statistics 23

viewing port statistics 23

viewing statistics 23

viewing test summary statistics 23

W

workflow of UHD 5

© Keysight Technologies, 2020–2021

Ixia, a Keysight Business
1400 Fountaingrove Parkway
Santa Rosa, CA 95403-1738