

Spirent Communications

# **Spirent TestCenter Software and Hardware New Features 5.13**

# Contents

<b>New Products and Features .....</b>	<b>3</b>
<b>Hardware Features .....</b>	<b>3</b>
<b>Software Features .....</b>	<b>4</b>
<b>Spirent Support .....</b>	<b>28</b>

# New Products and Features

## Hardware Features

### ***Support for 4x100G NRZ Breakouts on Spirent TestCenter 400G Appliances and Test Modules***



Spirent TestCenter 400G appliances and test modules now support 4x100G NRZ breakouts. With this new enhancement Spirent's 8-port 400G test systems become the industry's highest density 100G NRZ test systems.

This feature is supported on test modules purchased after February 2019 and appliances purchased after December 2019. To use the feature, the 400G system must support the 100G speed option. Purchase of ACC-1067 is required. This is an active copper cable that performs the 4x100G breakout. In addition, the appropriate software license is also required. On test modules this is BPK-1378 Enable QSFP-DD to 4XQSFP28 Base Package. On PX3 appliances it is HWO-PX3-QSFP-DD-8-4QSFP28 Spirent Hardware Option for PX3-QSFP-DD-8 400G to 4XQSFP28. On DX3 appliances this is HWO-DX3-QSFP-DD-8-4QSFP28 Spirent Hardware Option for DX3-QSFP-DD-8 400G to 4xQSFP28.

## Software Features

### ***LAG Support for 400G on PX3-QSFP-DD-8***

The Spirent TestCenter release notes for 5.11 noted that LAG for 400G ports was not supported on PX3-QSFP-DD-8 or DX3-QSFP-DD-8. With release 5.13, LAG for 400G ports is supported on the PX3-QSFP-DD-8 appliance.

### ***Priority Flow Control Measurements for 40G on PX3-QSFP28-12***

Spirent TestCenter allows testers to measure the time it takes for a device to pause after Spirent TestCenter sends a PFC pause frame (XOFF). It also measures the time it takes for the device to resume sending traffic after Spirent TestCenter sends a PFC frame requesting traffic be restarted (XON). The test system also evaluates the time the device actually paused compared to the time that Spirent TestCenter requested it to pause. These measurements are currently supported for 100G on PX3-QSFP28-12. With release 5.13 they are now supported at 40G as well. Knowledge Base article FAQ10225 outlines how to configure and use this feature.

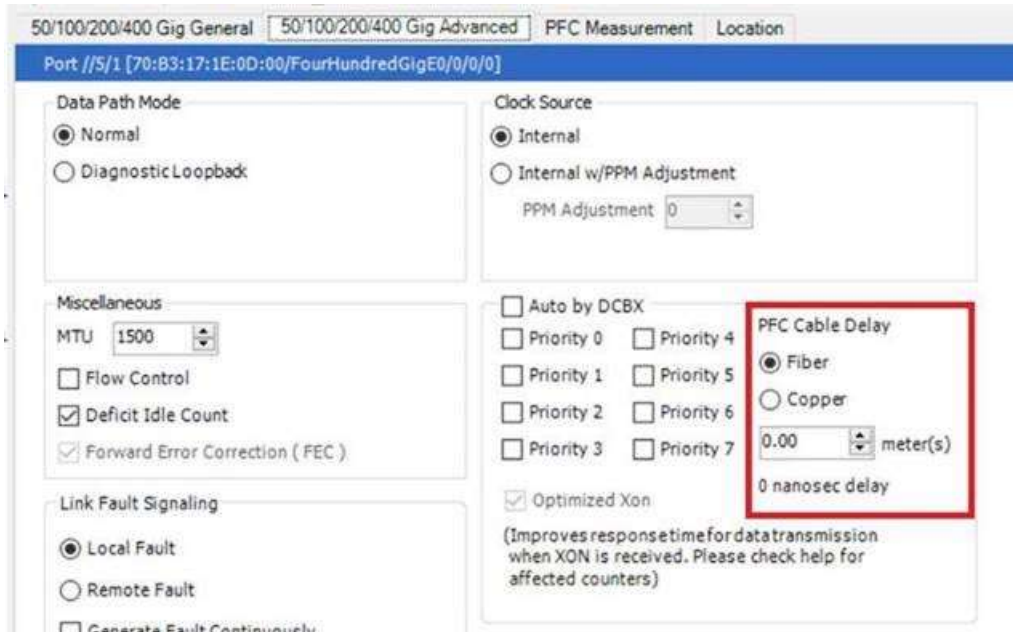
### ***User Defined Counters and User Defined Capture Counters for 40G on PX3-QSFP28-12***

Spirent TestCenter supports the configuration of counters based on our line-rate capture functionality. The user configures an offset in the frame to be analyzed by the capture subsystem as well as a byte pattern to be matched. During the test, all frames will be examined for the byte pattern at the particular offset. Matches will be counted and displayed in the results screens. This feature is frequently used to count frames that have particular addresses, particular configurations for QoS fields, or even particular values in the payload that might be relevant to a higher layer protocol. This feature is supported on PX3-QSFP28-12 modules in 100G mode. With release 5.13 it is now supported for 40G mode as well. Please see Knowledge Base article FAQ11000 for information about how to configure and use this feature.

### ***PFC Cable Delay Support for PX3-QSFP28-12***

This feature simulates the delay caused by long cables when using Priority Flow Control (PFC). When the device under test sends a pause frame to Spirent TestCenter, the response from Spirent TestCenter will be delayed by a certain amount of time to simulate the length of the cable between the DUT and Spirent TestCenter.

To access this feature, navigate to the port node in the Spirent TestCenter configuration tree of a PX3-QSFP28-12 port. The configuration settings are under the Advanced tab. The tester can choose to simulate either a fiber or copper cable of lengths up to 1 kilometer.



### **Custom Views - Persistence**

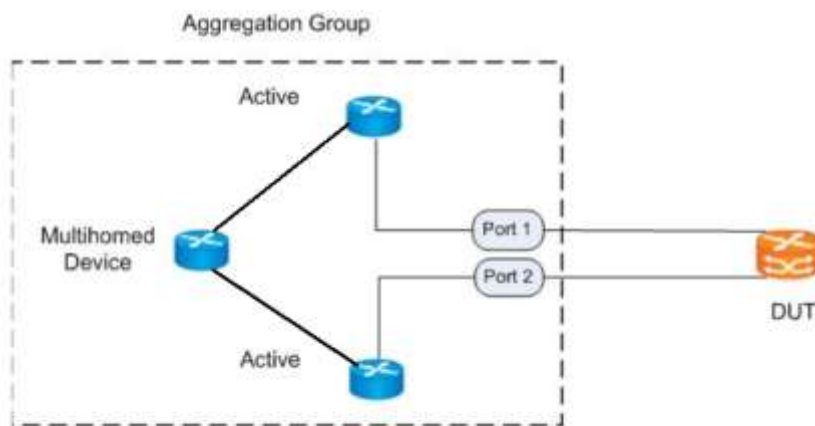
In release 5.11, we started an effort to ensure customized views are persistent across invocations of the Spirent TestCenter GUI. In release 5.11, the device configuration views were enhanced such that previously saved custom views were re-loaded when the application was restarted. In release 5.13, the stream block configuration views are also persistent across application launches.

### **ISISv6 MT-ID 0 support**

In Spirent TestCenter release 5.13, ISISv6 sessions can establish adjacency with MT-ID 0. Previously, ISISv6 sessions only supported MT-2. Now, you can configure MT-0 for ISISv6 session and establish session DUT. This support is important for a few ISIS SRv6 use cases. ISISv6 can still be configured with MT-2. There is no change in ISISv4 functionalities.

### **Active-Active Multihoming Control Plane support**

Spirent TestCenter release 5.13 introduces Active-Active multihoming support for IP Unicast and VPN routes. This is a significant improvement over the previous support of active-standby multihoming, where only one link could be active at one point in time. Now, control plane sessions can be brought up over multihomed links in true active-active fashion, where the control packet exchange over the links, and switchover in case of a failure, is completely dynamic. For example, BGP emulation can be multihomed behind ISIS emulation on multiple aggregated ports and connect to DUT via separate links. Link failure can be triggered on any of the links from the DUT side or within Spirent TestCenter. Control plane packet exchange will be switched over and remain uninterrupted over other active links. Therefore, no flap will be observed in the multihomed (BGP) session in case of a link failure.



### **Protocol Error Event Details**

Spirent TestCenter release 5.13 introduces an improved view for error event details. You access this view from the Event Dashboard by clicking on the error event tiles. This view contains detailed information for an event of error severity specific to the protocol, including session, routes, and FEC. This view can help speed up troubleshooting with all the additional information easily available in a single view. In release 5.13, this view is supported for BGP, EVPN, BGP SR/SRv6/SR-TE, BFD with ISIS, LDP, and RSVP as control plane.

### Error Events: BGP IPv4/v6 Routes

Events Dashboard

24 Events 24

**BGP Error**

8 Events

**BGP Down**

16 Events

---

BGP Error Event Details: BGP Error Show Acknowledged Events

Name	Device Name	Message	IPv4 Interface ...	IPv6 Interface ...	Error Code	Error Detail	Message Type	AFI	SAFI	MPLS Label	MPLS FEC
0.109.114.9...	Device_3	UPDATE Message E...	101.1.1.1	---	Invalid ORIGIN Atri...	Received + 86, expe...	UPDATE	IPv4	Labeled Unicast	100	Address = 12.1.1.0/24
0.109.114.9...	Device_3	UPDATE Message E...	101.1.1.1	---	Invalid ORIGIN Atri...	Received + 86, expe...	UPDATE	IPv4	Unicast	---	Address = 12.1.1.0/24
0.109.114.9...	Device_7	UPDATE Message E...	---	2002::1	Invalid ORIGIN Atri...	Received + 86, expe...	UPDATE	IPv6	Unicast	---	Address = 10.20.30.40.50.60.70.80/128
0.109.114.9...	Device_8	UPDATE Message E...	---	2003::1	Invalid ORIGIN Atri...	Received + 86, expe...	UPDATE	IPv6	Unicast	---	Address = 10.20.30.40.50.60.70.80/128
0.109.114.9...	Device_7	UPDATE Message E...	---	2002::1	Invalid ORIGIN Atri...	Received + 86, expe...	UPDATE	IPv6	Labeled Unicast	411	Address = 10.20.30.40.50.60.70.81/128
0.109.114.9...	Device_8	UPDATE Message E...	---	2003::1	Invalid ORIGIN Atri...	Received + 86, expe...	UPDATE	IPv6	Labeled Unicast	511	Address = 10.20.30.40.50.60.70.84/128
0.109.114.9...	Device_7	UPDATE Message E...	---	2002::1	Invalid ORIGIN Atri...	Received + 86, expe...	UPDATE	IPv6	Labeled VPN Unicast	412	Address = 10.20.30.40.50.60.70.82/128, RD = 5678:1234
0.109.114.8...	Device_3	UPDATE Message E...	---	2003::1	Invalid ORIGIN Atri...	Received + 86, expe...	UPDATE	IPv6	Labeled VPN Unicast	512	Address = 10.20.30.40.50.60.70.85/128, RD = 3456:2345

### Error Events: EVPN

Events Dashboard

4 Events 4

**BGP Error**

4 Events

---

BGP Error Event Details (Not Saved) Show Acknowledged Events

Device Name	IPv4 Interface...	IPv6 Interface ...	Message Type	AFI	SAFI	MPLS Label	MPLS FEC	Data Plane Encap...	Severity
BGP_IPv4_3_Port3	3.1.1.2	---	UPDATE	Layer-2 VPN	EVPN	600	Address = 3.1.1.1/32, RD = 10.1.1.3:1	MPLS	<span style="color: red;">!</span> Error
BGP_IPv4_2_Port2	2.1.1.2	---	UPDATE	Layer-2 VPN	EVPN	2000	Address = 10.00:00:00:00:02:48, RD = 10.1.1.2:1	VLAN	<span style="color: red;">!</span> Error
BGP_IPv6_1_Port3	---	2001::20	UPDATE	Layer-2 VPN	EVPN	7000	Address = 2001::3:0:34, RD = 10.1.1.A:1	VLAN	<span style="color: red;">!</span> Error
BGP_IPv6_1_Port2	1.1.1.2	---	UPDATE	Layer-2 VPN	EVPN	16	ESI = 06:0a:0a:0a:0a:00:00:00:00:00:00, RD = 10.1.1.1:1	MPLS	<span style="color: red;">!</span> Error

### Error Events: BGP SR/SRv6

BGP Error Event Details: BGP Error Show Acknowledged Events

Port Name	Device Name	Message	IPv4 Interface...	IPv6 Interface...	Error Code	Error Detail	Message Type	AFI	SAFI	MPLS Label	Severity
PortConfig2 v10.81...	R1_gw0	UPDATE Message E...	100.0.0.2	---	Unrecognized or Unsupported TLV in BGP Prot...	Unsupported TLV Type - Received = 6, Expecte...	UPDATE	IPv6	Labeled Unicast	14000	Auth
PortConfig2 v10.81...	R1_gw0	UPDATE Message E...	100.0.0.2	---	Malformed BGP Prefix 50 Address	Invalid Label Index TLV Length - Received = 0...	UPDATE	IPv6	Labeled Unicast	14000	Auth
PortConfig2 v10.81...	R2_gw0	UPDATE Message E...	---	2000::1:2	Unrecognized or Unsupported TLV in BGP Prot...	Unsupported TLV Type - Received = 7, Expecte...	UPDATE	IPv6	Labeled VPN Unicast	20	Auth
PortConfig2 v10.81...	R2_gw0	UPDATE Message E...	---	20001::2	Malformed IPv6 Service TLV	Invalid TLV Length - Received = 20, Expecte...	UPDATE	IPv6	Labeled VPN Unicast	20	Auth
PortConfig2 v10.81...	R1_gw0	UPDATE Message E...	100.0.0.2	---	Malformed BGP Prefix 50 Address	Invalid IPv6 TLV Length - Received = 6, Expecte...	UPDATE	IPv6	Labeled Unicast	14000	Auth
PortConfig2 v10.81...	R2_gw0	UPDATE Message E...	---	20001::2	Unrecognized or Unsupported TLV in BGP Prot...	Unsupported TLV Type - Received = 0, Expecte...	UPDATE	IPv6	Labeled VPN Unicast	19	Auth
PortConfig2 v10.81...	R2_gw0	UPDATE Message E...	---	20001::2	Malformed IPv6 Service TLV	Invalid TLV Length - Received = 21, Expecte...	UPDATE	IPv6	Labeled VPN Unicast	19	Auth
PortConfig2 v10.81...	R1_gw0	UPDATE Message E...	100.0.0.2	---	Malformed BGP Prefix 50 Address	Invalid IPv6 TLV Length - Received = 6, Expecte...	UPDATE	IPv6	Labeled Unicast	14000	Auth
PortConfig2 v10.81...	R1_gw0	UPDATE Message E...	100.0.0.2	---	Unrecognized or Unsupported TLV in BGP Prot...	Unsupported TLV Type - Received = 8, Expecte...	UPDATE	IPv6	Labeled Unicast	14000	Auth
PortConfig2 v10.81...	R1_gw0	UPDATE Message E...	100.0.0.2	---	Malformed BGP Prefix 50 Address	Invalid Label Index TLV Length - Received = 6...	UPDATE	IPv6	Labeled Unicast	14000	Auth

### Error Events: BGP SR-TE Policy

BGP Error Event Details: BGP Error Show Acknowledged Events

Port Name	Device Name	Message	IPv4 Interface...	IPv6 Interface...	Error Code	Error Detail	Message Type	AFI	SAFI	Severity
PortConfig2 v10.81...	R2	UPDATE Message Error	---	20001::2	Malformed SR Policy M/R	Invalid N/B Length - Received = 102, Expected = 66 or 162	UPDATE	IPv6	SR Policy	---
PortConfig2 v10.81...	R2	UPDATE Message Error	---	20001::2	Malformed SR Policy TLV	Invalid TLV Length - Received = 10, Expected = 11	UPDATE	IPv6	SR Policy	---
PortConfig2 v10.81...	R1	UPDATE Message Error	100.0.0.2	---	Malformed SR Policy M/R	Invalid N/B Length - Received = 90, Expected = 66 or 162	UPDATE	IPv6	SR Policy	---
PortConfig2 v10.81...	R1	UPDATE Message Error	100.0.0.2	---	Malformed SR Policy TLV	Invalid TLV Length - Received = 11, Expected = 12	UPDATE	IPv6	SR Policy	---

### Error Events: BFD over ISIS LSP

The screenshot shows the 'Events Dashboard' with 8 events. Three event cards are visible: 'BFD Down' (2 events), 'BFD Error' (4 events), and 'BFD Timer Expired' (2 events). Below the dashboard is a detailed table for 'BFD Error Event Details: BFD Error'.

Port Name	Device	Message	IPv4 Interface	Protocol Serial	FEC Type	FEC Info	My Discrimina...	Your Discrimin...	Severity
PortConfig1 //10.10...	ISIS_A	Authentication Fail...	192.85.1.3	ISIS	ISIS LSP	Prefix Address = 3.3.3.3, Prefix Length = 32	1111	3333	Error
PortConfig2 //10.10...	ISIS_B	Authentication Fail...	192.85.1.1	ISIS	ISIS LSP	Prefix Address = 1.1.1.1, Prefix Length = 32	3333	1111	Error
PortConfig1 //10.10...	ISIS_A	Authentication Fail...	192.85.1.3	ISIS	ISIS LSP	Prefix Address = 3.3.3.3, Prefix Length = 32	1111	3333	Error
PortConfig2 //10.10...	ISIS_B	Authentication Fail...	192.85.1.1	ISIS	ISIS LSP	Prefix Address = 1.1.1.1, Prefix Length = 32	3333	1111	Error

### Timer Error Events: BFD over LDP FEC

The screenshot shows the 'Events Dashboard' with 26 events. Four event cards are visible: 'LDP Down' (2 events), 'BFD Error' (8 events), 'LDP Error' (12 events), and 'BFD Timer Expired' (4 events). Below the dashboard is a detailed table for 'BFD Timer Expired Event Details: BFD Timer Expired'.

Port Name	Device Name	Message	IPv4 Interface	IPv6 Interface	Timer Value	Protocol Serial	FEC Type	FEC Info	My Discrimina...
Port //10.109.123.3...	PE Router (199.1.1.2)	Timer Expired	10.0.0.1	---	3000000 usecs	LDP	FEC 129	AGI Value = 220.30, Tail V...	10
Port //10.109.127.1...	PE Router (199.1.1.1)	Timer Expired	199.1.1.1	---	3000000 usecs	LDP	FEC 129	AGI Value = 220.30, Tail V...	10
Port //10.109.123.3...	PE Router (199.1.1.2)	Timer Expired	10.0.0.1	---	3000000 usecs	LDP	FEC 128	VC ID = 1, Endpoint ID = 0	10
Port //10.109.127.1...	PE Router (199.1.1.1)	Timer Expired	199.1.1.1	---	3000000 usecs	LDP	FEC 128	VC ID = 1, Endpoint ID = 0	10



### Event Details for Device Block

In Spirent TestCenter release 5.13, events can be identified for individual devices in a device block where the device count is more than 1. Information on the interface address IPv4/IPv6 is available and used for this purpose.

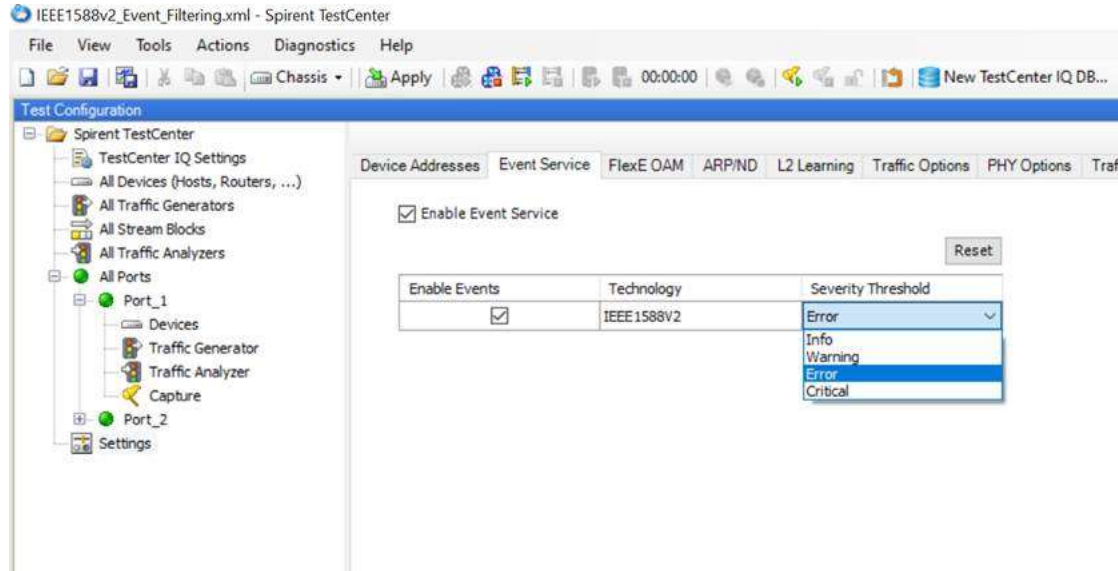


Port Name	Device Name	Message	IPv4 Interface Addr...	IPv6 Interface Addr...	Severity	Protocol Session Ty...
Port //10.109.114.91/1/1	Device_2	Authentication Failure	101.1.2.1	—	Error	BGP
Port //10.109.114.91/1/1	Device_2	Authentication Failure	101.1.1.1	—	Error	BGP
Port //10.109.124.157/1/1	Device_1	Authentication Failure	101.1.2.2	—	Error	BGP
Port //10.109.124.157/1/1	Device_1	Authentication Failure	101.1.1.2	—	Error	BGP
Port //10.109.114.91/1/1	Device_4	Authentication Failure	—	2003::1	Error	BGP
Port //10.109.114.91/1/1	Device_4	Authentication Failure	—	2002::1	Error	BGP
Port //10.109.124.157/1/1	Device_3	Authentication Failure	—	2003::2	Error	BGP
Port //10.109.124.157/1/1	Device_3	Authentication Failure	—	2002::2	Error	BGP
Port //10.109.114.91/1/1	Device_6	Authentication Failure	200.1.1.1	—	Error	OSPFv2
Port //10.109.124.157/1/1	Device_5	Authentication Failure	200.1.1.2	—	Error	OSPFv2
Port //10.109.114.91/1/1	Device_6	Authentication Failure	200.1.2.1	—	Error	OSPFv2
Port //10.109.124.157/1/1	Device_5	Authentication Failure	200.1.2.2	—	Error	OSPFv2
Port //10.109.124.157/1/1	Device_5	Authentication Failure	200.1.1.2	—	Error	OSPFv2
Port //10.109.114.91/1/1	Device_6	Authentication Failure	200.1.1.1	—	Error	OSPFv2

## Protocol Event Filter

In Spirent TestCenter release 5.13, you can control which protocol events to publish from their respective daemons and filter out unimportant events from a test. From the Event Service options available in Global Settings, you can select a protocol and severity threshold to publish the events for the same. Any configured protocol will be automatically listed here and available for selection. Event filter is supported for Routing, SDN, Data Center, and TSN protocols.

This will significantly improve the user experience through a decluttered Events view, with fewer events and more focused debugging during the test.



## LDP Protocol Events

In Spirent TestCenter release 5.13, LDP protocol events are supported and can be viewed in Spirent TestCenter IQ. LDP events help troubleshoot any test involving LDP emulation. For LDP protocol, the available events are described below.

LDP Up and Down events are generated when protocol state changes to up or down.



The screenshot shows the 'Events Timespan View' in Spirent TestCenter IQ. The table displays a list of events, including several 'LDP Up' events. The columns are: Event Name, Time Stamp, Severity, Message, Source, Category, Detailed Name, Device Name, and Error Code.

Event Name	Time Stamp	Severity	Message	Source	Category	Detailed Name	Device Name	Error Co
Test Start	2020-07-13 3:25:08...	Info		STC	Test Events	com.spirent.stc.eve...	---	---
Apply Start	2020-07-13 3:25:14...	Info		STC	Test Events	com.spirent.stc.eve...	---	---
Apply Complete	2020-07-13 3:25:18...	Info		STC	Test Events	com.spirent.stc.eve...	---	---
Start All Devices	2020-07-13 3:25:18...	Info		STC	Test Events	com.spirent.stc.eve...	---	---
LDP Up	2020-07-13 3:25:28...	Info	LDP Device Up	STC://10.109.123.3/...	Protocol Events	com.spirent.stc.eve...	Device A_5	---
LDP Up	2020-07-13 3:25:28...	Info	LDP Device Up	STC://10.109.127.1...	Protocol Events	com.spirent.stc.eve...	Device B_6	---
LDP Up	2020-07-13 3:25:29...	Info	LDP Device Up	STC://10.109.123.3/...	Protocol Events	com.spirent.stc.eve...	Device A_5	---
LDP Up	2020-07-13 3:25:29...	Info	LDP Device Up	STC://10.109.127.1...	Protocol Events	com.spirent.stc.eve...	Device B_5	---
LDP Up	2020-07-13 3:25:30...	Info	LDP Device Up	STC://10.109.127.1...	Protocol Events	com.spirent.stc.eve...	Device B_8	---
LDP Up	2020-07-13 3:25:30...	Info	LDP Device Up	STC://10.109.123.3/...	Protocol Events	com.spirent.stc.eve...	Device A_8	---

LDP Error/Warning events are generated when any unexpected error occurred during test. This could be due to malformed packets or unsupported protocol attributes received from the DUT.

Event Name	Severity	Message	Dev...	Error Detail
Command: LDP Se...	Info	LDP Send Custom PDUs	LDP_V4,1	---
LDP Error	Warning	Missing Message Parameter	LDP_V4,2	Received TLV = Unknown TLV. Expected Mandatory TLV = FEC TLV. in the Beginning of Label Request Message
LDP Error	Warning	Missing Message Parameter	LDP_V4,2	---
Apply Start	Info	---	---	---
Apply Complete	Info	---	---	---
Command: LDP Se...	Info	LDP Send Custom PDUs	LDP_V4,1	---
LDP Down	Error	LDP device is down due to error	LDP_V4,2	---
LDP Down	Info	LDP device is down due to command execution	LDP_V4,1	---
LDP Error	Error	Bad Message Length	LDP_V4,2	Received Invalid Length For Message Type = Label Request Message
LDP Error	Error	Shutdown	LDP_V4,1	Received SHUTDOWN notification TLV from LDP peer
LDP Up	Info	LDP Device Up	LDP_V4,2	---
LDP Up	Info	LDP Device Up	LDP_V4,1	---

LDP Command events are generated when a user invokes commands to trigger changes in protocol behavior during the test.

Event Name	Time Stamp	Severity	Message	Source	Category	Detailed Name	Device Name
Command: LDP Res...	2020-07-13 3:28:43	Info	LDP Resume Keepalives	STC//10.109.123.3/...	Protocol Events	com.spirent.stc.eve...	Device_A_1
Command: LDP Res...	2020-07-13 3:28:43	Info	LDP Resume Keepalives	STC//10.109.123.3/...	Protocol Events	com.spirent.stc.eve...	Device_A_10
Command: LDP Res...	2020-07-13 3:28:43	Info	LDP Resume Keepalives	STC//10.109.123.3/...	Protocol Events	com.spirent.stc.eve...	Device_A_9
Command: LDP Res...	2020-07-13 3:28:43	Info	LDP Resume Keepalives	STC//10.109.123.3/...	Protocol Events	com.spirent.stc.eve...	Device_A_8
Command: LDP Res...	2020-07-13 3:28:43	Info	LDP Resume Keepalives	STC//10.109.123.3/...	Protocol Events	com.spirent.stc.eve...	Device_A_7
Command: LDP Res...	2020-07-13 3:28:43	Info	LDP Resume Keepalives	STC//10.109.123.3/...	Protocol Events	com.spirent.stc.eve...	Device_A_6
Command: LDP Res...	2020-07-13 3:28:43	Info	LDP Resume Keepalives	STC//10.109.123.3/...	Protocol Events	com.spirent.stc.eve...	Device_A_5
Command: LDP Res...	2020-07-13 3:28:43	Info	LDP Resume Keepalives	STC//10.109.123.3/...	Protocol Events	com.spirent.stc.eve...	Device_A_4
Command: LDP Res...	2020-07-13 3:28:43	Info	LDP Resume Keepalives	STC//10.109.123.3/...	Protocol Events	com.spirent.stc.eve...	Device_A_3
Command: LDP Res...	2020-07-13 3:28:43	Info	LDP Resume Keepalives	STC//10.109.123.3/...	Protocol Events	com.spirent.stc.eve...	Device_A_2
Command: LDP Wit...	2020-07-13 3:28:49	Info	LDP Withdraw Mac Addresses	STC//10.109.123.3/...	Protocol Events	com.spirent.stc.eve...	Device_A_1
Command: LDP Wit...	2020-07-13 3:28:49	Info	LDP Withdraw Mac Addresses	STC//10.109.127.1/...	Protocol Events	com.spirent.stc.eve...	Device_B_1

LDP Timer events are generated when any of the protocol timer expires during test.

Event Name	Time Stamp	Severity	Message	Source	Device Name	Error Detail	Timer Name	Timer Reason	Timer Value
LDP Timer Expired	2020-07-13 3:28:26	Error	Timer Expired	STC//10.109.123.3/...	Device_A_4	---	Holding Timer Expir...	---	45 secs
LDP Timer Expired	2020-07-13 3:28:26	Error	Timer Expired	STC//10.109.123.3/...	Device_A_10	---	Holding Timer Expir...	---	45 secs
LDP Timer Expired	2020-07-13 3:28:27	Error	Timer Expired	STC//10.109.123.3/...	Device_A_9	---	Holding Timer Expir...	---	45 secs
LDP Timer Expired	2020-07-13 3:28:27	Error	Timer Expired	STC//10.109.123.3/...	Device_B_8	---	Holding Timer Expir...	---	45 secs
LDP Timer Expired	2020-07-13 3:28:27	Error	Timer Expired	STC//10.109.127.1/...	Device_B_7	---	Holding Timer Expir...	---	45 secs
LDP Timer Expired	2020-07-13 3:28:28	Error	Timer Expired	STC//10.109.127.1/...	Device_B_2	---	Holding Timer Expir...	---	45 secs
LDP Timer Expired	2020-07-13 3:28:30	Error	Timer Expired	STC//10.109.123.3/...	Device_A_6	---	Holding Timer Expir...	---	45 secs
LDP Timer Expired	2020-07-13 3:28:30	Error	Timer Expired	STC//10.109.127.1/...	Device_A_2	---	Holding Timer Expir...	---	45 secs
LDP Timer Expired	2020-07-13 3:28:30	Error	Timer Expired	STC//10.109.123.3/...	Device_A_2	---	Holding Timer Expir...	---	45 secs
LDP Timer Expired	2020-07-13 3:28:31	Error	Timer Expired	STC//10.109.123.3/...	Device_A_2	---	Holding Timer Expir...	---	45 secs
LDP Timer Expired	2020-07-13 3:28:36	Error	Timer Expired	STC//10.109.123.3/...	Device_A_9	---	Holding Timer Expir...	---	45 secs
LDP Timer Expired	2020-07-13 3:28:37	Error	Timer Expired	STC//10.109.127.1/...	Device_B_8	---	Holding Timer Expir...	---	45 secs

### IGMP/MLD Protocol Events

In Spirent TestCenter release 5.13, IGMP/MLD protocol events are supported and can be viewed in Spirent TestCenter IQ. IGMP/MLD events help troubleshoot any test involving IGMP/MLD emulation. For IGMP/MLD protocol, the available events are described below.

IGMP/MLD Up and Down events are generated when protocol state changes to up or not started.

Event Name	Time Stamp	Severity	Message	Source	Device Name	Port Name
IGMP Up	2020-07-13 07:30:01	Info	IGMP Host Up	STC//10.109.126.158/11	SwiStack Client 1	Port 0/10/126.158/11
IGMP Up	2020-07-13 07:30:01	Info	IGMP Host Up	STC//10.109.126.158/11	SwiStack Client 2	Port 0/10/126.158/11
IGMP Up	2020-07-13 07:30:01	Info	IGMP Host Up	STC//10.109.126.158/11	SwiStack Client 1	Port 0/10/126.158/11
IGMP Up	2020-07-13 07:30:01	Info	IGMP Host Up	STC//10.109.126.158/11	SwiStack Client 2	Port 0/10/126.158/11
IGMP Down	2020-07-13 07:45:39	Info	IGMP Host Down	STC//10.109.126.158/11	SwiStack Client 2	Port 0/10/126.158/11
IGMP Down	2020-07-13 07:45:40	Info	IGMP Host Down	STC//10.109.126.158/11	SwiStack Client 1	Port 0/10/126.158/11
IGMP Down	2020-07-13 07:45:39	Info	IGMP Host Down	STC//10.109.126.158/11	SwiStack Client 1	Port 0/10/126.158/11
IGMP Down	2020-07-13 07:45:39	Info	IGMP Host Down	STC//10.109.126.158/11	SwiStack Client 2	Port 0/10/126.158/11

Event Name	Time Stamp	Severity	Message	Source	Device Name	Port Name
MLD Up	2020-07-18 09:40:59	Info	MLD Host Up	STC-170.108.126.170/1	Switch-Client-1	Port-170.108.126.170/1
MLD Up	2020-07-18 09:41:30	Info	MLD Host Up	STC-170.108.126.170/1	Switch-Client-2	Port-170.108.126.170/1

Event Name	Time Stamp	Severity	Message	Source	Device Name	Port Name
MLD Down	2020-07-18 09:44:51	Info	MLD Host Down	STC-170.108.126.170/1	Switch-Client-2	Port-170.108.126.170/1
MLD Down	2020-07-18 09:44:51	Info	MLD Host Down	STC-170.108.126.170/1	Switch-Client-1	Port-170.108.126.170/1

IGMP/MLD Error events are generated when any unexpected error occurred during the test. This could be due to malformed packet or unsupported protocol attribute received from the DUT.

Event Name	Time Stamp	Severity	Message	Source	Device Name	Port Name
IGMP Error	2020-07-18 09:27:36.774	Error	Message Header Error	STC-170.108.126.170/1	Ingress Message Classifier	Classifier-1-Device1
IGMP Error	2020-07-18 09:27:57.513	Error	Message Header Error	STC-170.108.126.170/1	Ingress Message Classifier	Type-Mismatch-2-16
IGMP Error	2020-07-18 09:27:57.013	Error	Malformed Address Error	STC-170.108.126.170/1	Ingress Multicast Address	Group-Address-1-1.1.1.1
IGMP Error	2020-07-18 09:28:05.799	Error	Join Group Error	STC-170.108.126.170/1	Device-2	No-Traffic-For-Multicast-Group

Event Name	Time Stamp	Severity	Message	Source	Device Name	Port Name
MLD Error	2020-07-18 09:34:29.490	Error	Message Header Error	STC-170.108.126.170/1	Ingress Message Classifier	Classifier-1-Device1
MLD Error	2020-07-18 09:34:29.473	Error	Join Group Error	STC-170.108.126.170/1	Device-2	No-Traffic-For-Multicast-Group
MLD Error	2020-07-18 09:34:38.713	Error	Join Group Error	STC-170.108.126.170/1	Device-2	Group-Address-1-16.2

IGMP/MLD Command events are generated when user invoke commands like join, leave, rejoin, start, stop, etc., to trigger changes in protocol behavior during the test.

Event Name	Time Stamp	Severity	Message	Source	Device Name	Port Name
Command IGMP Join Group	2020-07-18 09:40:49.490	Info	Join 1 group(s)	STC-170.108.126.170/1	Switch-Client-1	Port-170.108.126.170/1
Command IGMP Join Group	2020-07-18 09:40:50.930	Info	Join 1 group(s)	STC-170.108.126.170/1	Switch-Client-2	Port-170.108.126.170/1
Command IGMP Leave Group	2020-07-18 09:41:15.1	Info	Leave 1 group(s)	STC-170.108.126.170/1	Switch-Client-2	Port-170.108.126.170/1
Command IGMP Leave Group	2020-07-18 09:41:55.9	Info	Leave 1 group(s)	STC-170.108.126.170/1	Switch-Client-1	Port-170.108.126.170/1

Event Name	Time Stamp	Severity	Message	Source	Device Name	Port Name
Command IGMP Stop Querier	2020-07-18 09:22:03.941	Info	Stop IGMP Querier	STC-170.108.126.170/1	Switch-Client-1	Port-170.108.126.170/1
Command IGMP Start Querier	2020-07-18 09:22:13.061	Info	Start IGMP Querier	STC-170.108.126.170/1	Switch-Client-1	Port-170.108.126.170/1
Command IGMP Stop Querier	2020-07-18 09:22:18.081	Info	Stop IGMP Querier	STC-170.108.126.170/1	Switch-Client-1	Port-170.108.126.170/1

Event Name	Time Stamp	Severity	Message	Source	Device Name	Port Name
Command MLD Join Group	2020-07-18 09:40:49.490	Info	Join 1 group(s)	STC-170.108.126.170/1	Switch-Client-1	Port-170.108.126.170/1
Command MLD Join Group	2020-07-18 09:40:50.930	Info	Join 1 group(s)	STC-170.108.126.170/1	Switch-Client-2	Port-170.108.126.170/1
Command MLD Leave Group	2020-07-18 09:41:15.1	Info	Leave 1 group(s)	STC-170.108.126.170/1	Switch-Client-1	Port-170.108.126.170/1
Command MLD Leave Group	2020-07-18 09:41:54.9	Info	Leave 1 group(s)	STC-170.108.126.170/1	Switch-Client-2	Port-170.108.126.170/1

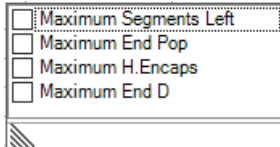
Event Name	Time Stamp	Severity	Message	Source	Device Name	Port Name
Command MLD Stop Querier	2020-07-18 09:22:03.941	Info	Stop MLD Querier	STC-170.108.126.170/1	Switch-Client-1	Port-170.108.126.170/1
Command MLD Stop Querier	2020-07-18 09:22:03.941	Info	Stop MLD Querier	STC-170.108.126.170/1	Switch-Client-2	Port-170.108.126.170/1

## ISIS SRv6 Control Plane Draft Update

Spirent TestCenter release 5.13 added support for the latest IETF ISIS SRv6 draft <https://tools.ietf.org/html/draft-ietf-lsr-isis-srv6-extensions-07>.

The draft update includes:

- New MSD types in the SR Link Node MSD Sub TLVs are added



- New “Sid Structure Sub TLV” is added to SRv6 End SID, SRv6 End.X SID and SRv6 LAN End.X SID Sub-TLVs.

Name	Device Name	LAN	Flags	Algorithm	Weight	Endpoint Behavior	Enable Custom Endpoint Behavior	SID	ISIS Custom sub-TLVs	LB Length	LN Length	Function Length	Argument Length
IsisSrv6NeighborConfig 2	Device 1	32y...					<input checked="" type="checkbox"/>						
IsisSrv6EndSidSubTlv 2					100	End.X (no P...	<input checked="" type="checkbox"/>	aaa:1:1:1::	1 sub-TLV	32	32	32	32
IsisSrv6SidStructureSubTlv 3							<input checked="" type="checkbox"/>						

Name	Device Name	LAN	Flags	Algorithm	Weight	Endpoint Behavior	Enable Custom Endpoint Behavior	SID	ISIS Custom sub-TLVs	LB Length	LN Length	Function Length	Argument Length
IsisSrv6NeighborConfig 2	Device 2						<input checked="" type="checkbox"/>						
IsisSrv6LanEndXsidSubTlv 1				0	200	End.X (no P...	<input checked="" type="checkbox"/>	aaa:1:1:1::	1 sub-TLV	32	32	32	32
IsisSrv6SidStructureSubTlv 3							<input checked="" type="checkbox"/>						

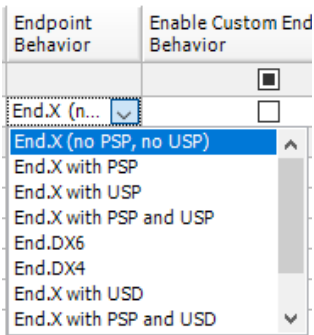
  

Name	Active	MT ID	Metric	Flags	Algorithm	Number of Locators	Locator Size	Locator	Locator Increment	ISIS Custom sub-TLVs	Flags	Endpoint Behavior	Enable Custom End Behavior
IsisSrv6LocatorTlv 2	<input checked="" type="checkbox"/>	0	10		0	1	64	aaa:1:1:1::	1	1 sub-TLV		End (no PSP...	<input checked="" type="checkbox"/>
IsisSrv6EndSidSubTlv 2	<input checked="" type="checkbox"/>												<input checked="" type="checkbox"/>
IsisSrv6SidStructureSubTlv 3	<input checked="" type="checkbox"/>												<input checked="" type="checkbox"/>

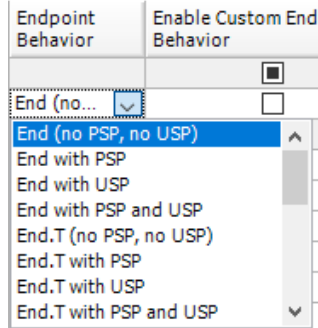
- SRv6 Locator TLV now supports multiple locator entries

Neighbor	L2 Bundle Neighbor	IPv4 Routes	IPv6 Routes	PLSB Instance	PLSB ISID Address	Capability TLV	MAC Reachability TLV	Group Add
Name	Active	MT ID	Metric	Flags	Algorithm	Number of Locators	Locator Size	Locator
IsisSrv6LocatorTlv 2	<input checked="" type="checkbox"/>	0	10		0	10	64	aaa:1:1:1::
IsisSrv6EndSidSubTlv 2	<input checked="" type="checkbox"/>							
IsisSrv6SidStructureSubTlv 3	<input checked="" type="checkbox"/>							

- Node SID and Link SID now have separate endpoint behavior lists.



Endpoint Behavior List of Link SID



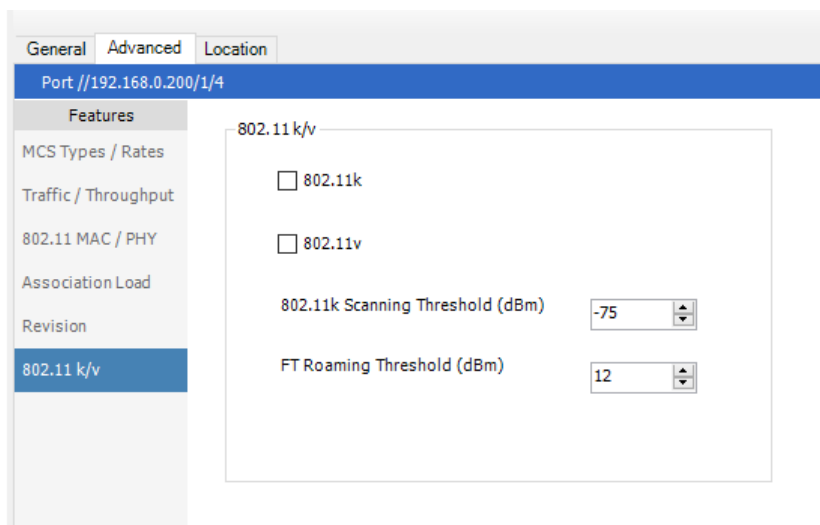
Endpoint Behavior List of Node SID

### 802.11 k/v FT Roaming

In Spirent TestCenter release 5.13, 802.11 k/v roaming is enabled, so an emulated client can perform roaming among APs that support 802.11 k/v roaming protocols. This new feature is now supported on all Spirent Wi-Fi 6 platforms as listed below.

Part Number	Description
C50-KIT-11AX-1-V2	C50 W/ 4-PORT 10G/5G/2.5G/1G/100M Copper, 802.11ax Wi-Fi NICs, 2.4GHz/5GHz, Internal Attenuation, DFS Radar Signal Emulation, HW Timing
C50-KIT-11AX-3	C50 4-Port 10G/5G/2.5G/1G/100M Copper, One 802.11AX Wi-Fi NIC, 2.4GHZ/5GHZ, Internal Attenuation and HW Timing
MX2-11AX-2-V2	MX2 Test Module with 802.11ax Wi-Fi, 2.4GHz/5GHz, Internal Attenuation, DFS Radar Signal Emulation, and Hardware Timing
AP-C2-KIT-11AX-1	C2 4-Port 10G/5G/2.5G/1G/100M Copper, One 802.11AX Wi-Fi NIC, 2.4GHZ/5GHZ, Internal Attenuation and HW Timing C50 4-Port 10G/5G/2.5G/1G/100M Copper, 802.11AX Wi-Fi NICs for 20 OFDMA/MU Clients, 2x2 MIMO, 2.4GHz/5GHz, and HW Timing
C50-KIT-11AX-6	C50 4-Port 10G/5G/2.5G/1G/100M Copper, 802.11AX Wi-Fi NICs for 20 OFDMA/MU Clients, 2x2 MIMO, 2.4GHz/5GHz, and HW Timing

11r roaming is already supported; now all 802.11 k/v/r roaming are supported for fast transition inter-AP roaming testing. As shown in the following screen capture, 802.11 k/v roaming for emulated clients is disabled by default. It must be manually enabled to activate the feature before an association process. 802.11k and 802.11v can be enabled or disabled independently.



A new set of Wi-Fi statistics called “IEEE 802.11 Neighbor Report” is created to support 802.11v roaming processing. This will provide details of available targeted APs for 802.11v roaming purposes.

Port Name	Client Mac Address	AP SSID	AP BSSID	RSSI

It is known that 802.11v BSS Transition Message (BTM) has the following types:

- Query (Client): Client’s Query to request a BSS transition management requesting a BSS transition candidate list to its associated AP
- Request (AP): An AP responds to a BTM Query frame with a BTM request frame
- Response (Client): A Response frame by a client back to the AP to inform whether it accepts or denies the transmission

Therefore, a set of new statistics are added as listed below specifically for 802.11v roaming:

- BTM Query Count (Frames)
- BTM Request Count (Frames)
- BTM Response Accept Count (Frames)
- BTM Response Denial Count (Frames)

Along with the existing roaming timing and counter statistics and metrics can be used as shown:

- Fast Transition Type
- Fast Transition Successful Counter
- Fast Transition Failure Counter
- Fast Transition Average Delay (ms)
- Fast Transition Delay (ms)
- Fast Transition Maximum Delay (ms)
- Fast Transition Minimum Delay (ms)

Port Name	Fast Transition BSSID	BTM Query Count (Frames)	BTM Request Count (Frames)	BTM Response Accept Count (Frames)	BTM Response Denial Count (Frames)	Fast Transition Average Delay (ms)	Fast Transition Delay (ms)	Fast Transition Failure	Fast Transition Success	Fast Transition Maximum Delay (ms)	Fast Transition Minimum Delay (ms)	Fast Transition Successful	Fast Transition Type
Port_1/19	00:00:00:00:00:00	0	0	0	0	0	0	0	0	0	0	0	N/A
Port_1/18	00:00:00:00:00:00	0	0	0	0	0	0	0	0	0	0	0	N/A
Port_1/17	00:00:00:00:00:00	0	0	0	0	0	0	0	0	0	0	0	N/A
Port_1/16	00:00:00:00:00:00	0	0	0	0	0	0	0	0	0	0	0	N/A
Port_1/15	00:00:00:00:00:00	0	0	0	0	0	0	0	0	0	0	0	N/A
Port_1/14	00:00:00:00:00:00	0	0	0	0	0	0	0	0	0	0	0	N/A
Port_1/13	00:00:00:00:00:00	0	0	0	0	0	0	0	0	0	0	0	N/A
Port_1/12	00:00:00:00:00:00	0	0	0	0	0	0	0	0	0	0	0	N/A
Port_1/11	00:00:00:00:00:00	0	0	0	0	0	0	0	0	0	0	0	N/A
Port_1/10	00:00:00:00:00:00	0	0	0	0	0	0	0	0	0	0	0	N/A
Port_1/9	00:00:00:00:00:00	0	0	0	0	0	0	0	0	0	0	0	N/A
Port_1/8	00:00:00:00:00:00	0	0	0	0	0	0	0	0	0	0	0	N/A
Port_1/7	00:00:00:00:00:00	0	0	0	0	0	0	0	0	0	0	0	N/A

802.11 k/v/r is a licensed feature with these license part numbers.

Part Number	Description	Platform
BPK-5007	802.11 K/V/R Support for Spirent TestCenter	Test Module
C50-BPK-5007	802.11 K/V/R Support for Spirent TestCenter C50	C50
AP-BPK-5007	802.11 K/V/R Support for Spirent TestCenter C2	C2

### Wi-Fi Noise Generation

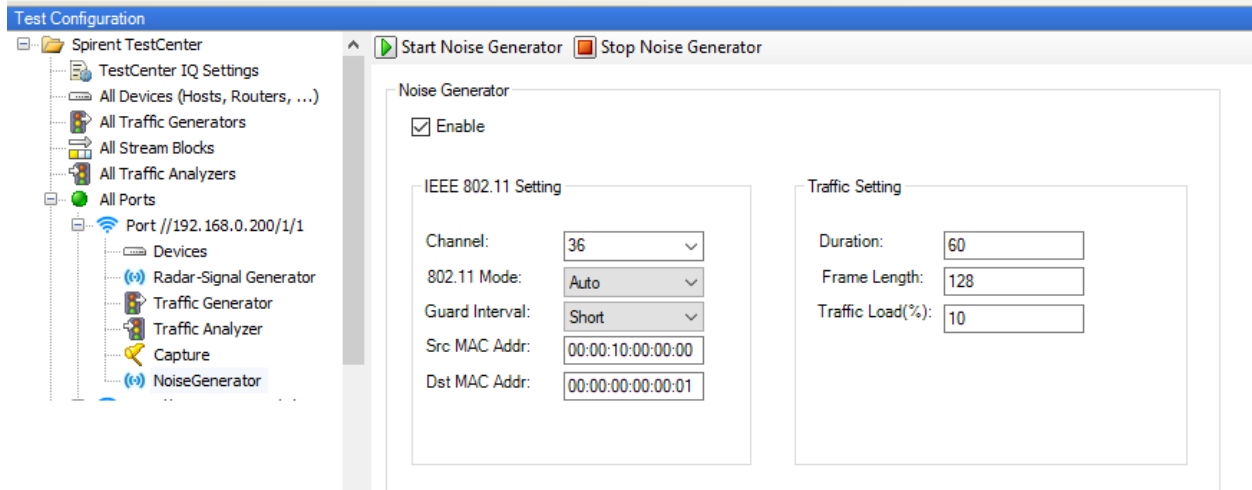
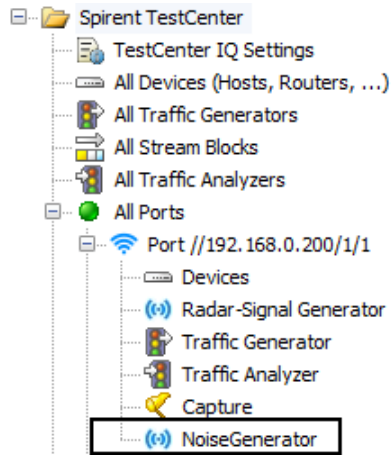
A Wi-Fi Noise Generation feature is added with the Spirent TestCenter 5.13 release. The feature is for the following non-HRC Wi-Fi 6 platforms:

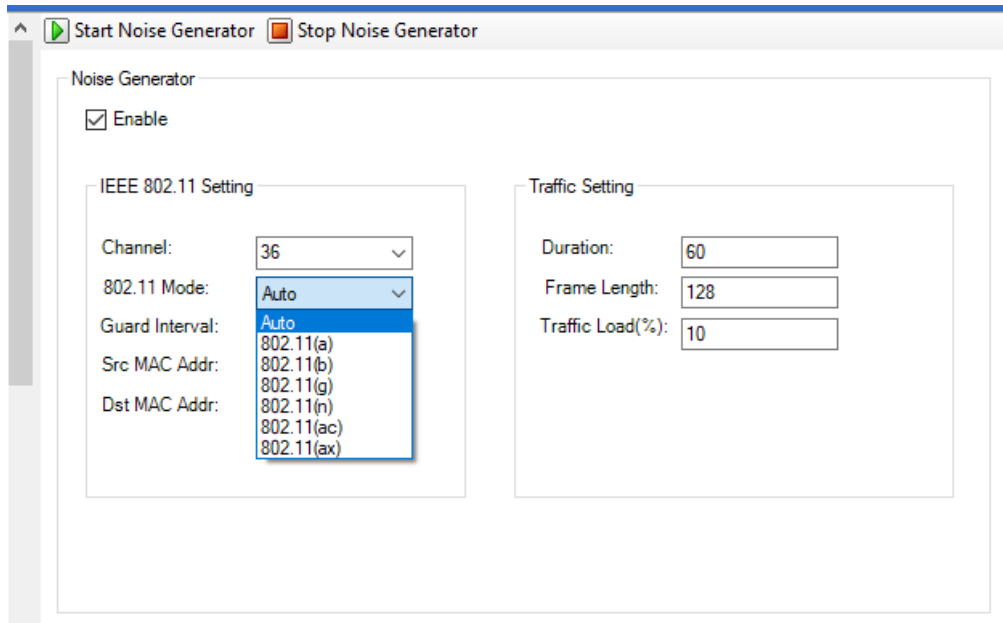
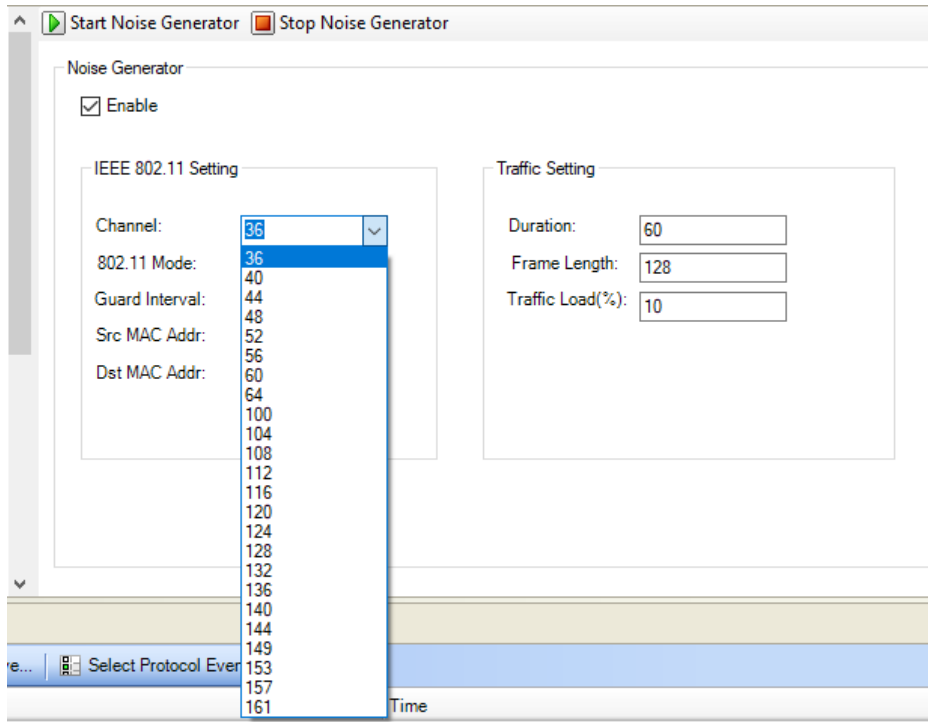
Part Number	Description
C50-KIT-11AX-1-V2	C50 W/ 4-PORT 10G/5G/2.5G/1G/100M Copper, 802.11ax Wi-Fi NICs, 2.4GHZ/5GHZ, Internal Attenuation, DFS Radar Signal Emulation, HW Timing
C50-KIT-11AX-3	C50 4-Port 10G/5G/2.5G/1G/100M Copper, One 802.11AX Wi-Fi NIC, 2.4GHZ/5GHZ, Internal Attenuation and HW Timing
MX2-11AX-2-V2	MX2 Test Module with 802.11ax Wi-Fi, 2.4GHZ/5GHZ, Internal Attenuation, DFS Radar Signal Emulation, and Hardware Timing
AP-C2-KIT-11AX-1	C2 4-Port 10G/5G/2.5G/1G/100M Copper, One 802.11AX Wi-Fi NIC, 2.4GHZ/5GHZ, Internal Attenuation and HW Timing

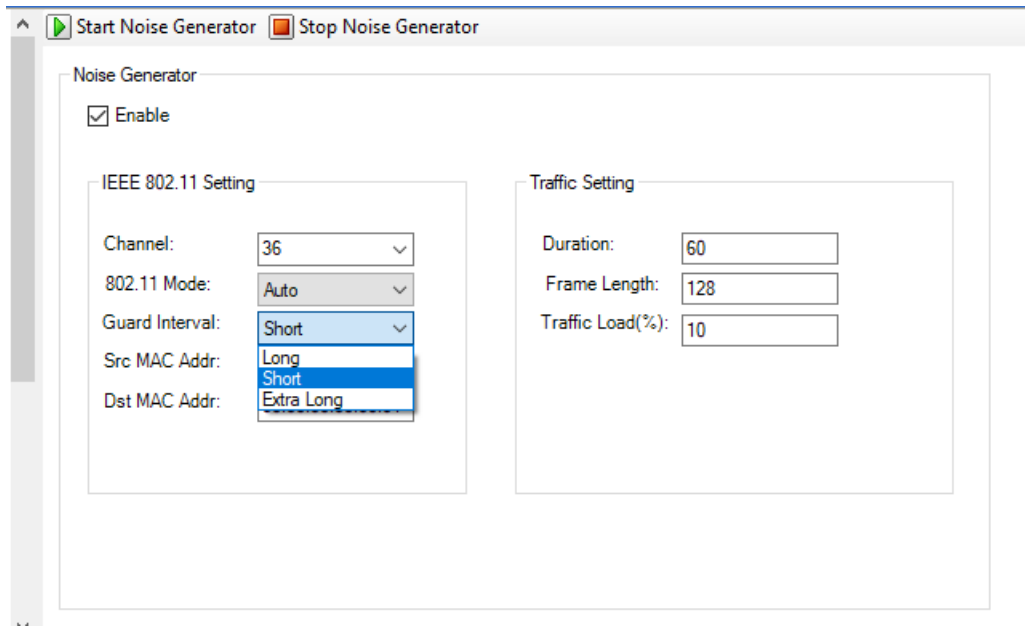
Wi-Fi noise generation needs to allocate a Wi-Fi radio interface for Wi-Fi traffic transmission without an association or connection with an AP. At this point, Wi-Fi noise generation transmits out normal Wi-Fi traffic subject to Wi-Fi CSMA/CD contention mechanism with a pre-configured Wi-Fi PHY and MAC layer such as channel, 802.11 mode, GI, MCS type, etc., along with desired traffic. The port level configuration for the Wi-Fi radio interface is still completely applicable while a port is selected for the noise generation purpose. The example use cases for this new Wi-Fi noise generation are for co-channel and adjunct channel traffic co-existing testing.



The configuration UI for the new Wi-Fi noise generation is shown in the screen captures:







The Wi-Fi Noise Generation feature requires the following license to operate.

Part Number	Description	Platform
BPK-5006	Wi-Fi Noise Generation for Spirent TestCenter	Test Module
C50-BPK-5006	Wi-Fi Noise Generation for Spirent TestCenter C50	C50
AP-BPk-5006	Wi-Fi Noise Generation for Spirent TestCenter C2	C2

## Calculate and Display Disk Usage for Spirent TestCenter IQ

Spirent TestCenter provides estimates for how much disk space will be used by Spirent TestCenter IQ results for a given test, based on the test configuration. The calculated size is an estimate and depends on the number of metrics selected for collection, the collection frequency, number of ports and streams, as well as the length of the test. If a test configuration is modified, users can get an updated estimate by clicking "Calculate" after applying the new configuration.

Result Selector

Test Information

Enable TestCenter IQ

Live Results Database Size Calculator

Enter test duration in minutes:  Calculate

Projected db size is: 6.06 MB

i Calculation based on live results. Snapshots increase actual db size. Unapplied configuration changes are not included in the projection.

Live Data Management

Configuration and Learned Properties

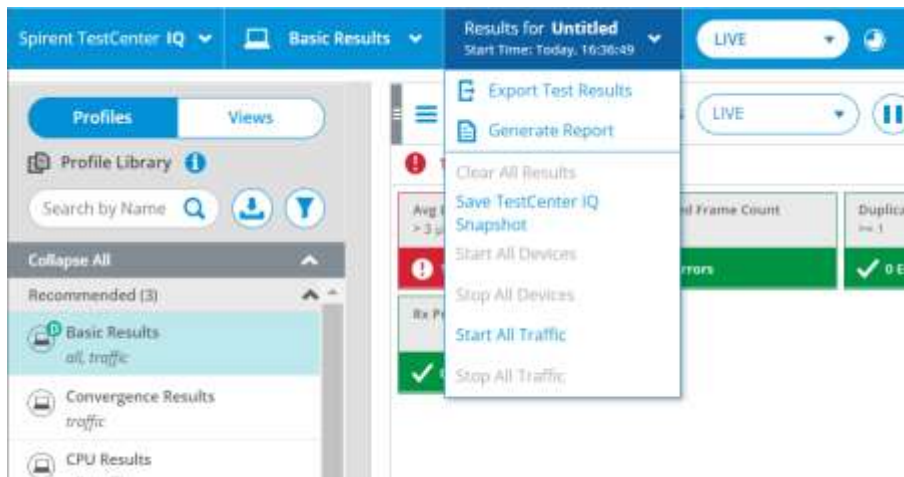
Limit live result data saved to:  minutes  
 Limit current test db storage to :  GB

Result Group (366 Selected)	Collection Interval (ms)
<ul style="list-style-type: none"> <li> <input checked="" type="checkbox"/> L1               <ul style="list-style-type: none"> <li><input checked="" type="checkbox"/> L1 FEC Symbol Error Histogram</li> <li><input checked="" type="checkbox"/> L1 Lane PCS/FEC</li> <li><input checked="" type="checkbox"/> L1 Lane PRBS PAM4</li> <li><input checked="" type="checkbox"/> L1 Lane Transceiver</li> <li><input checked="" type="checkbox"/> L1 Lane Transceiver Eyescan</li> <li><input checked="" type="checkbox"/> L1 Port</li> </ul> </li> <li> <input checked="" type="checkbox"/> L2L3               <ul style="list-style-type: none"> <li><input type="checkbox"/> Port Basic</li> <li><input checked="" type="checkbox"/> Port CPU</li> <li><input type="checkbox"/> Gbu Results</li> <li><input type="checkbox"/> Gbv Results</li> <li><input checked="" type="checkbox"/> Stream</li> </ul> </li> </ul>	<ul style="list-style-type: none"> <li>1,000</li> <li>1,000</li> <li>1,000</li> <li>1,000</li> <li>1,000</li> <li>1,000</li> <li>1,000</li> <li>1,000</li> <li>1,000</li> <li>1,000</li> <li>1,000</li> <li>1,000</li> <li>1,000</li> <li>1,000</li> <li>1,000</li> <li>1,000</li> </ul>

## Spirent TestCenter Actions Menu in TestCenter IQ

Spirent TestCenter IQ platform now supports adding application actions directly to the TestCenter IQ web UI. In release 5.13, new menu items have been added to the top action menu. Users can now invoke the following six actions from the TestCenter IQ UI.

- Clear All Results
- Save TestCenter IQ Snapshot
- Start All Devices
- Stop All Devices
- Start All Traffic
- Stop All Traffic



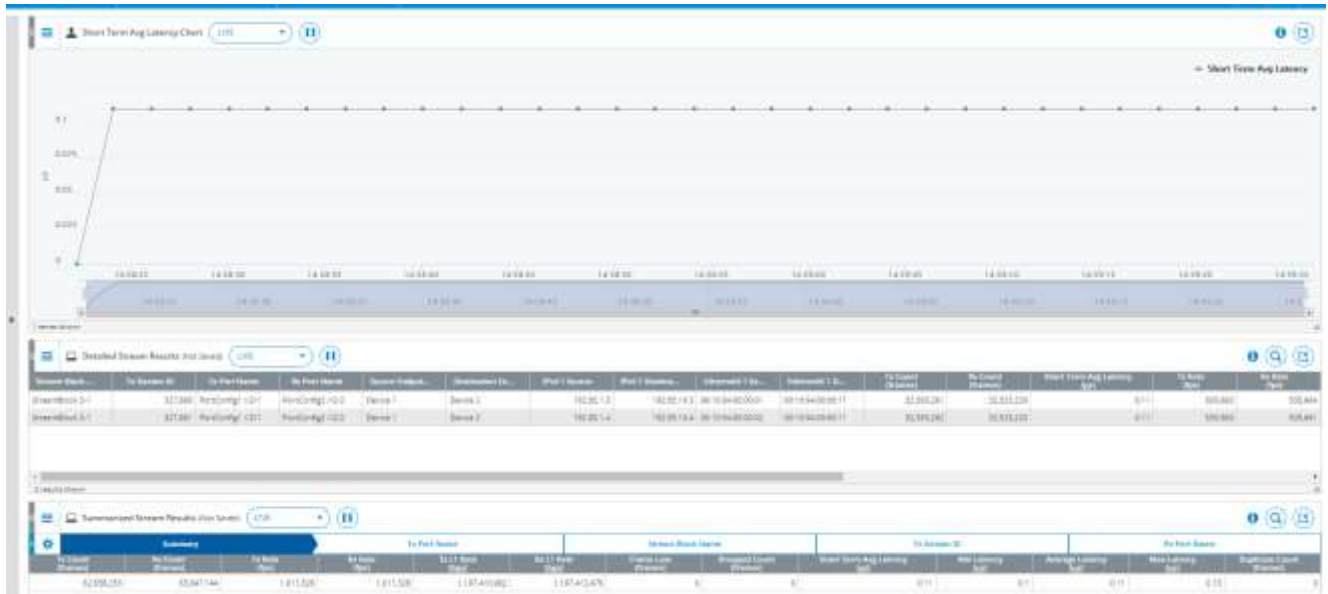
This convenience feature allows users to access commonly used actions directly from the web UI instead of switching back and forth between TestCenter IQ and Spirent TestCenter GUI.

## DUT Events Support

Spirent TestCenter IQ includes a robust Events feature that allows users to view events from Spirent hardware and software. Users can get GUI notifications via special alert icons and Event Dashboard views. Release 5.13 expands the Events feature to include DUT/SUT-generated events. TestCenter IQ now includes a SNMP trap collector that can receive SNMP traps from DUTs and convert them to Events that can be shown in TestCenter IQ tables and graphs. These events can be displayed on the dashboard, sorted, correlated, plotted on graphs, and filtered, just like Spirent TestCenter generated events. A complete list of supported MIBs and traps is available at [DOC12030](#) on the Spirent Customer Service Center (CSC) website.

### Short Term Latency Support

Spirent TestCenter hardware modules support measuring short term latency values. This support has now been added to TestCenter IQ. Similar to other latency metrics, short-term latency values can now be displayed in tables and plotted on a time-series chart. It has been added to the detailed stream results view by default as well.



### Spirent TestCenter Bulk ReST APIs

Spirent TestCenter Bulk ReST APIs are a series of ReST API functions designed for Spirent TestCenter object management in bulk. Four bulk ReST APIs are introduced in release 5.13: bulk create, bulk read, bulk configure, and bulk delete.

Using Spirent TestCenter bulk ReST APIs, users can create, configure, and delete multiple Spirent TestCenter objects in one or a few ReST calls, to improve the efficiency of testing and regression.

An example of performance improvement: to configure an attribute of 1000 devices, previously, 1000 Spirent TestCenter config ReST calls had to be invoked, now only one Spirent TestCenter bulkconfig ReST call is needed; this table shows a sample test result.

<b>API Function</b>	<b>Windows client – LabServer (via ReST API)</b>
Previous Spirent TestCenter config ReST API	16366ms (1000 ReST calls)
New Spirent TestCenter bulk config ReST API	784ms (1 ReST call)
Performance improved: approximately <b>21 times faster</b>	

Additionally, xpath expression is introduced in Spirent TestCenter bulk ReST APIs. By using xpath expression, users can easily find out an object via its attribute(s) and make changes on the object in one ReST call. Below is a curl example to configure the router ID of a device which name is "router1":

```
curl -g -X PUT -H "X-STC-API-Session:Session01" -d routerid=2.2.2.2
http://10.109.118.119/stcapi/bulk/objects/emulateddevice[name^=router1]
```

Please refer to Chapter 4 in the *Spirent TestCenter Automation Programmer's Reference* for more examples.

Spirent TestCenter bulk ReST API is only available in Spirent TestCenter LabServer, it is not supported in Stcweb.

### **Enhanced L4-7: New Hardware Support**

- Added support for C2 appliance (10G Quint speed NIC (NIC-63) Only).
- Added support for NIC-47 (FX2 10/1G Ethernet SFP+ NIC 4-PORT) used in C50
- For the latest list of supported hardware, refer to [FAQ18968](#).

### **Enhanced L4-7: Virtual Machine Support**

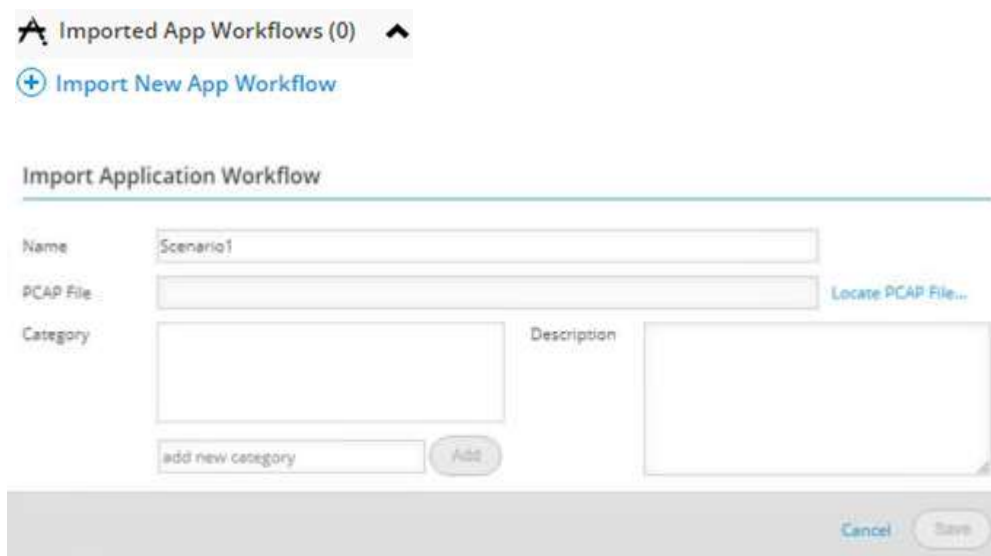
Added support for Spirent TestCenter AWS Virtual Machine (V-FMT-AWS)

### **Enhanced L4-7: Application Import / Playback**

Application Import and Playback (AIP) allows the user to import a PCAP file and create L4-7 traffic from one or more of the streams available within that file.

AIP is also supported on LabServer

A PCAP of the application is first imported. Click Import New App Workflow to open a new window where you can configure the location of the pcap file and select the required streams.



Imported App Workflows (0) ▲

⊕ Import New App Workflow

Import Application Workflow

Name: Scenario1

PCAP File: [Empty] Locate PCAP File...

Category: [Empty] add new category Add

Description: [Empty]

Cancel Save

After loading the PCAP file, you can view the streams available within the PCAP file and select the ones you want to use. Source and Destination IP address and Port numbers are listed. After saving the configuration, any of those streams may be selected for playback..

Import Application Workflow

Name:

PCAP File:  [Locate PCAP File...](#)

Category:  Description:

Streams: Packet Delay:  Close Type:

Include	Source	Source Port	Destination	Destination Port
<input checked="" type="checkbox"/>	10.40.60.44	1687	64.4.60.7	80
<input checked="" type="checkbox"/>	10.40.60.44	1688	64.4.60.7	80
<input checked="" type="checkbox"/>	10.40.60.44	1689	10.40.50.228	135
<input checked="" type="checkbox"/>	10.40.60.44	1690	10.40.50.228	5002

The Packet Delay pull-down menu is used to override the individual packet delays that are stored in each stream file. The following options are available:

- Preserve (default): Attempt to preserve the original timing, as indicated in the data file.
- None: No delay. Send packets as soon as possible.
- Custom: Use specified delay in milliseconds for all packets.
- Minimum: Use specified minimum delay in milliseconds, or the times in the data file, if they are longer.

### ***Enhanced L4-7: Spirent TestCenter IQ Events Support***

Spirent TestCenter IQ Events are now generated at Start Test, Stop Test, Abort Test, and at the start of the Ramp Up, Steady, and Ramp Down phases of L4-7 traffic generation.

### ***Enhanced L4-7: Persistent Bandwidth Health Indicators***

A new health indicator shows red at the end of the test, if the test failed to reach the assigned bandwidth during the steady phase of the test.

### ***Enhanced L4-7: Average Bandwidth During Steady Phase of Traffic Generation***

It is now possible to measure the average bandwidth achieved during the steady state phase of traffic generation.

### ***Enhanced L4-7: Test Report Support***

The user may now generate a PDF test report containing the Enhanced L4-7 test configuration, results table, and graphs from the test execution.

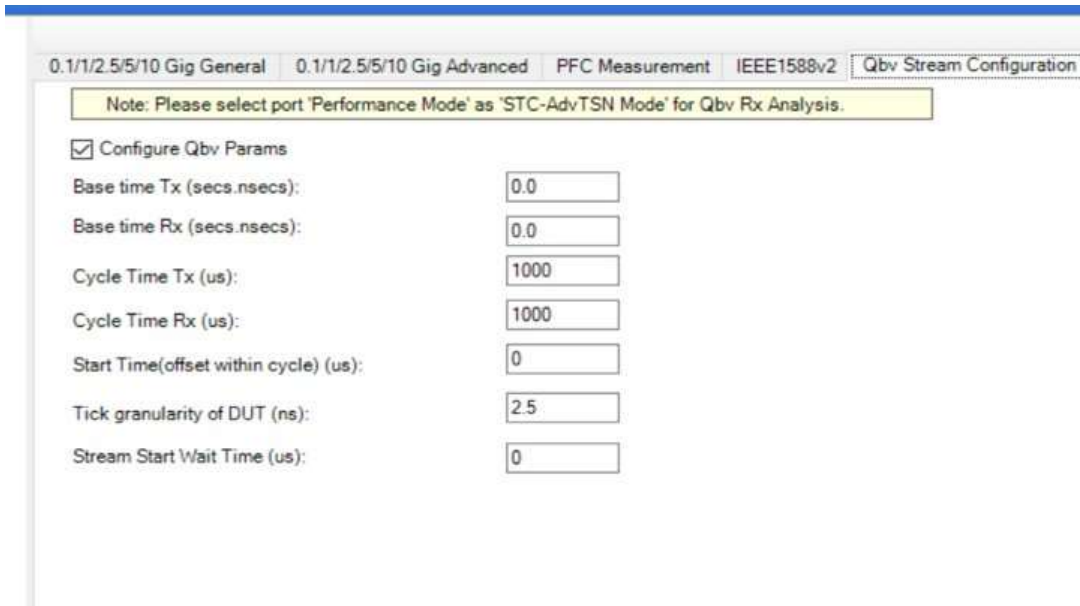


### TSN Protocols: QBV Common Across IEEE1588v2 and IEEE8021AS

Use this feature to send QBV Streams from both IEEE1588v2 and IEEE8021AS. QBV RX Analysis is also possible from both IEEE1588v2 and IEEE8021AS. Ports should be in STC\_ADVTSN mode.

The following screen captures highlight the new configuration options and sequencer commands. The existing Qbv functionality is unchanged.

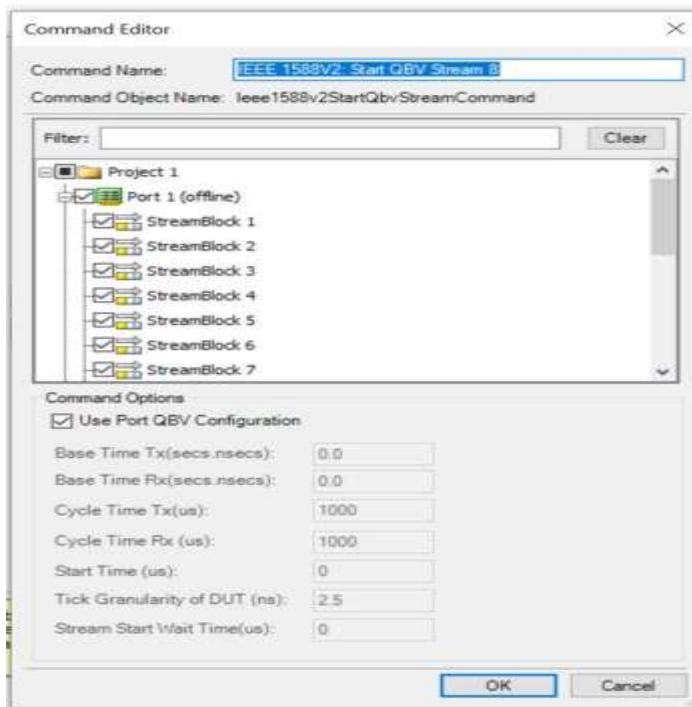
#### Qbv Configuration



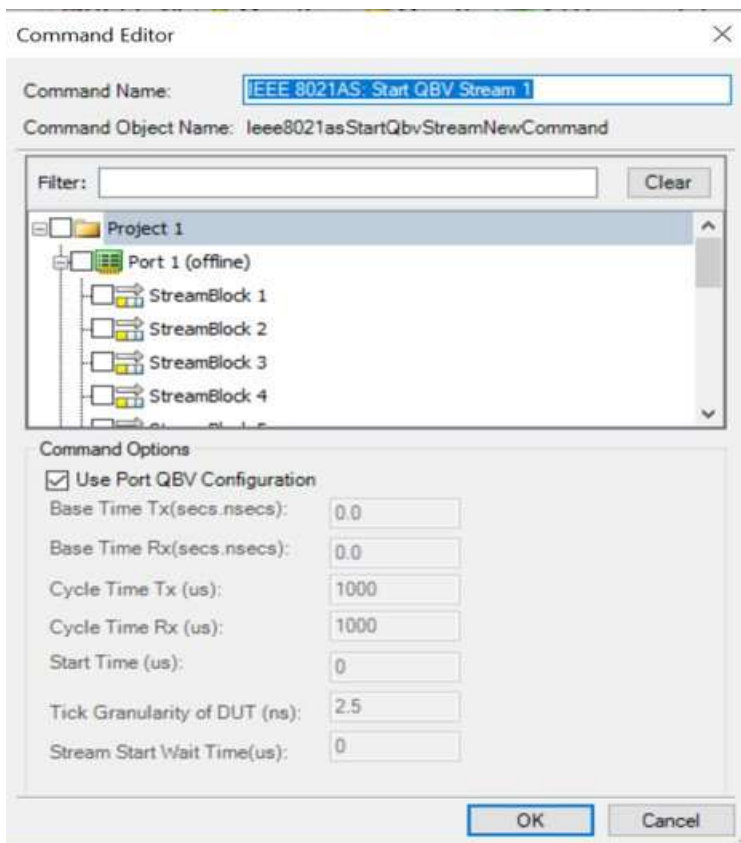
#### QBV Start Command from IEEE1588v2



Sequencer Command: QBV Start Command from IEEE1588v2



Sequencer Command: QBV Start Command from IEEE821AS



### TSN Protocols: IEEE1588v2 Rx Delay Response Rate for Specific Slaves

Delay response meant for every other slave is also received by each slave. Previously, the results displayed the overall rate of delay response messages received. This enhancement added new result fields to show the rate of delay response messages meant only for a particular slave in Multicast mode.

- In IEEE1588v2 Message Results, these new fields are added:
  - > Rx Min Slave Specific Delay Response Rate (Packets Per Second)
  - > Rx Max Slave Specific Delay Response Rate (Packets Per Second)
  - > Rx Avg Slave Specific Delay Response Rate (Packets Per Second)
- These fields specify Rx Delay Response Rate for Per Slave in Multicast Mode.
  - > IEEE1588v2 Message Rates

Carrier Ethernet > IEEE 1588v2 Results > IEEE 1588v2 Message Rate Results | Change Result View | Manage Profiles... | IEEE 802.11 | 1 of 1 | Show: All Ports

Port Name	Device Name	Tags	Device	Rx Max Delay Response Rate (Packets Per Second)	Rx Avg Delay Response Rate (Packets Per Second)	Rx Min Slave Specific Delay Response Rate (Packets Per Second)	Rx Max Slave Specific Delay Response Rate (Packets Per Second)	Rx Avg Slave Specific Delay Response Rate (Packets Per Second)
Port 1	Device 1	Clic...	1	0	0	0	0	0
Port 2	Device 2	Clic...	1	2.002	1.927	1	1	1
Port 2	Device 3	Clic...	1	2.002	1.927	1	1.001	1

# Spirent Support

To obtain technical support for Spirent Communications products, please contact our Support Services department using any of the following methods:

## **Americas**

E-mail: [support@spirent.com](mailto:support@spirent.com)

Web: <https://support.spirent.com>

Toll Free: +1 800-SPIRENT (+1 800-774-7368) (North America)

Phone: +1 818-676-2616

Hours: Monday through Friday, 05:00 to 17:00 Pacific Time

## **Europe, Middle East, Africa**

E-mail: [support@spirent.com](mailto:support@spirent.com)

Web: <https://support.spirent.com>

Phone: +33 (1) 6137 2270 (France)

Phone: +44 1803 546333 (UK)

Hours: Monday through Thursday, 09:00 to 18:00, 9:00 to 17:00 Friday, Paris Time

## **Asia Pacific**

E-mail: [support@spirent.com](mailto:support@spirent.com)

Web: <https://support.spirent.com>

Phone: +86 (400) 810-9529 (toll-free mainland China only)

Phone: +86 (10) 8233 0033 (China)

Operating Hours: Monday through Friday, 09:00 to 18:00 Beijing Time

## **Company Address**

Spirent Communications, Inc.  
27349 Agoura Road  
Calabasas, CA 91301  
USA

The latest versions of user manuals, application notes, and software and firmware updates are available on the Spirent Communications Customer Service Center website at <https://support.spirent.com>.

Information about Spirent Communications and its products and services can be found on the company website at <https://www.spirent.com>.

© 2020 All of the company names and/or brand names and/or product names referred to in this document, in particular, the name "Spirent" and its logo device, are either registered trademarks or trademarks of Spirent plc and its subsidiaries, pending registration in accordance with relevant national laws. All other registered trademarks or trademarks are the property of their respective owners.