H3C S5560X-EI Product Test Procedures

Statement

This Test procedure is only used to describe possible security issues. Without the permission of H3C Security, the content of this test procedure may not be modified or added or deleted, and it may not be used for commercial purposes in any way. Any direct or indirect consequences and losses caused by the dissemination and use of the information provided in this security bulletin shall be the responsibility of the user himself. The New H3C Security and the author of the security bulletin shall not bear any responsibility for this. The New H3C Security has the right to modify and interpret this test procedure. If you want to reprint or disseminate this test procedure, you must ensure the integrity of this test procedure, including all content such as the copyright statement.

Revision Record

Date	Revision Version	Sec No.	Change Description	Author

Contents

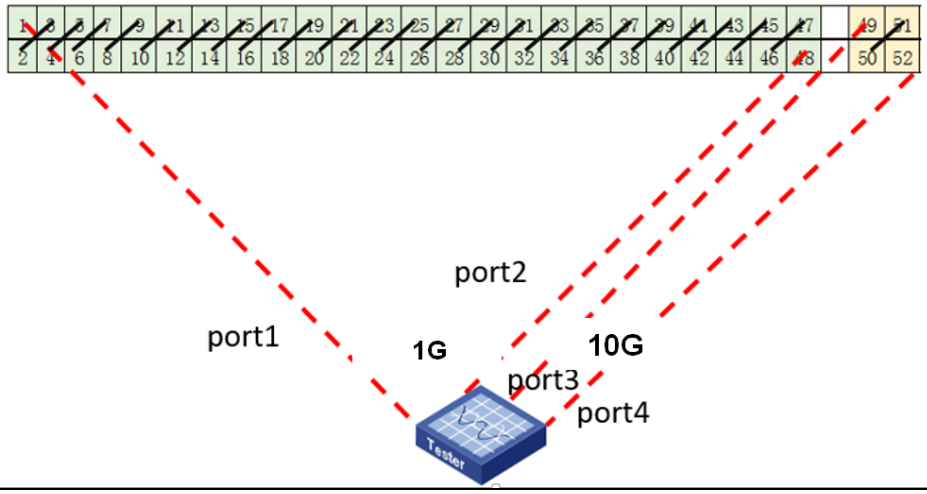
1 Performance test

1.1 Layer 2 forwarding performance

Test Item Name: Layer 2 forwarding performance

Work Hour: 120 min

Test Topology:



Test Process:

1. Use the Tester to send IPv4 Layer 2 unicast traffic at wire speed to the DUT.
2. The packet destination is the other port on the tester.
3. Use packets of 64 bytes, 128 bytes, 256 bytes, 512 bytes, 1024 bytes, 1280 bytes, and 1518 bytes for the tests.
4. Each test is no shorter than 120 seconds.
5. Record the packet loss, throughput, and latency statistics. Result 1 is expected.

Expect Results:

1. The switch achieves 100% throughput and no packet loss.

Actual Result:

1. Disable stp globally.

```
[DUT]undo stp global enable
```

2. Enter tclsh view to configure vlan and all ports by using scripts.

```
<DUT>tclsh
<DUT-tcl>
```

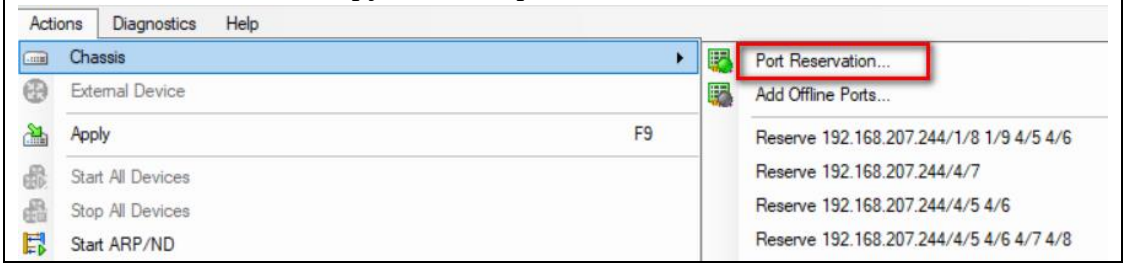
```
[DUT-tcl]vlan 1 to 26
[DUT-tcl]for {set i 2} {$i<=24} {incr i} {
     interface  GigabitEthernet1/0/[expr $i*2-1]
      port access vlan  [expr $i]
    interface  GigabitEthernet1/0/[expr $i*2]
      port access vlan [expr $i]
}
[DUT-tcl]for {set i 25} {$i<=26} {incr i} {
     interface  Ten-GigabitEthernet  1/0/[expr $i*2-1]
      port access vlan  [expr $i]
     interface  Ten-GigabitEthernet  1/0/[expr $i*2]
      port access vlan [expr $i]
}
```

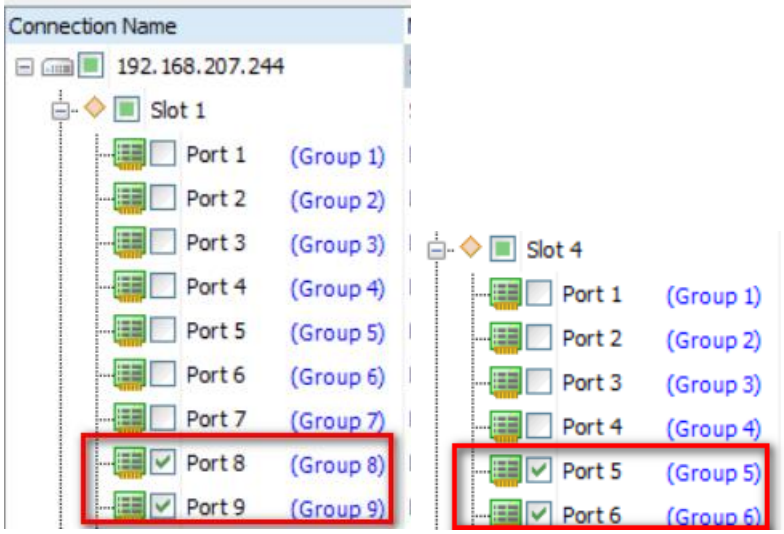
3. Check vlan on each ports by inputting command *display interface brief*.

```
Brief information on interfaces in bridge mode:
Link: ADM - administratively down; Stby - standby
Speed: (a) - auto
Duplex: (a)/A - auto; H - half; F - full
Type: A - access; T - trunk; H - hybrid
Interface            Link Speed   Duplex Type PVID Description
GE1/0/1              UP   1G(a)   F(a)   A    1
GE1/0/2              UP   1G(a)   F(a)   A    1
GE1/0/3              UP   1G(a)   F(a)   A    2
GE1/0/4              UP   1G(a)   F(a)   A    2
GE1/0/5              UP   1G(a)   F(a)   A    3
GE1/0/6              UP   1G(a)   F(a)   A    3
GE1/0/7              UP   1G(a)   F(a)   A    4
GE1/0/8              UP   1G(a)   F(a)   A    4
GE1/0/9              UP   1G(a)   F(a)   A    5
GE1/0/10             UP   1G(a)   F(a)   A    5
GE1/0/11             UP   1G(a)   F(a)   A    6
GE1/0/12             UP   1G(a)   F(a)   A    6
GE1/0/13             UP   1G(a)   F(a)   A    7
GE1/0/14             UP   1G(a)   F(a)   A    7
GE1/0/15             UP   1G(a)   F(a)   A    8
GE1/0/16             UP   1G(a)   F(a)   A    8
GE1/0/17             UP   1G(a)   F(a)   A    9
GE1/0/18             UP   1G(a)   F(a)   A    9
GE1/0/19             UP   1G(a)   F(a)   A    10
GE1/0/20             UP   1G(a)   F(a)   A    10
GE1/0/21             UP   1G(a)   F(a)   A    11
GE1/0/22             UP   1G(a)   F(a)   A    11
GE1/0/23             UP   1G(a)   F(a)   A    12
GE1/0/24             UP   1G(a)   F(a)   A    12
```

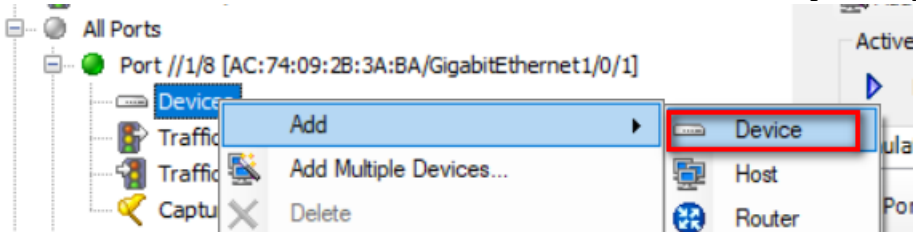
```
GE1/0/25              UP   1G(a)   F(a)   A    13
GE1/0/26              UP   1G(a)   F(a)   A    13
GE1/0/27              UP   1G(a)   F(a)   A    14
GE1/0/28              UP   1G(a)   F(a)   A    14
GE1/0/29              UP   1G(a)   F(a)   A    15
GE1/0/30              UP   1G(a)   F(a)   A    15
GE1/0/31              UP   1G(a)   F(a)   A    16
GE1/0/32              UP   1G(a)   F(a)   A    16
GE1/0/33              UP   1G(a)   F(a)   A    17
GE1/0/34              UP   1G(a)   F(a)   A    17
GE1/0/35              UP   1G(a)   F(a)   A    18
GE1/0/36              UP   1G(a)   F(a)   A    18
GE1/0/37              UP   1G(a)   F(a)   A    19
GE1/0/38              UP   1G(a)   F(a)   A    19
GE1/0/39              UP   1G(a)   F(a)   A    20
GE1/0/40              UP   1G(a)   F(a)   A    20
GE1/0/41              UP   1G(a)   F(a)   A    21
GE1/0/42              UP   1G(a)   F(a)   A    21
GE1/0/43              UP   1G(a)   F(a)   A    22
GE1/0/44              UP   1G(a)   F(a)   A    22
GE1/0/45              UP   1G(a)   F(a)   A    23
GE1/0/46              UP   1G(a)   F(a)   A    23
GE1/0/47              UP   1G(a)   F(a)   A    24
GE1/0/48              UP   1G(a)   F(a)   A    24
XGE1/0/49             UP   10G(a)  F(a)   A    25
XGE1/0/50             UP   10G(a)  F(a)   A    25
XGE1/0/51             UP   10G(a)  F(a)   A    26
```

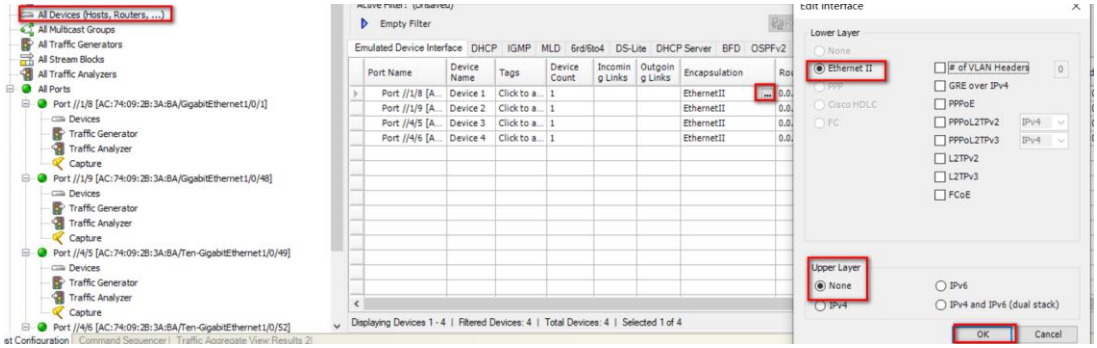
4. Connect TC and occupy the tester port.



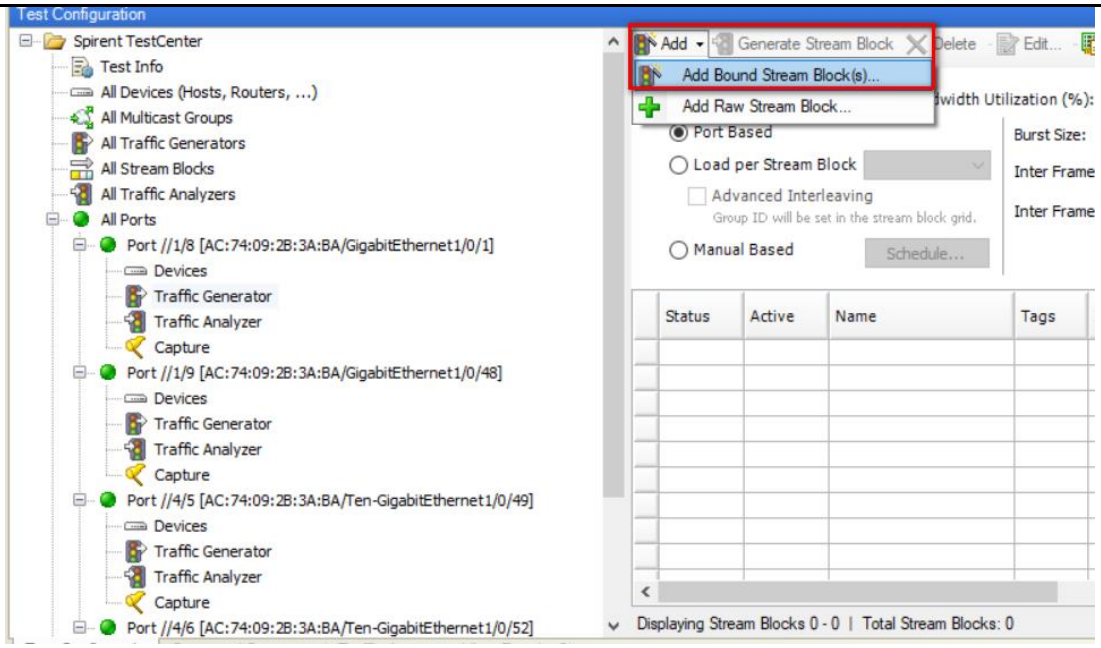


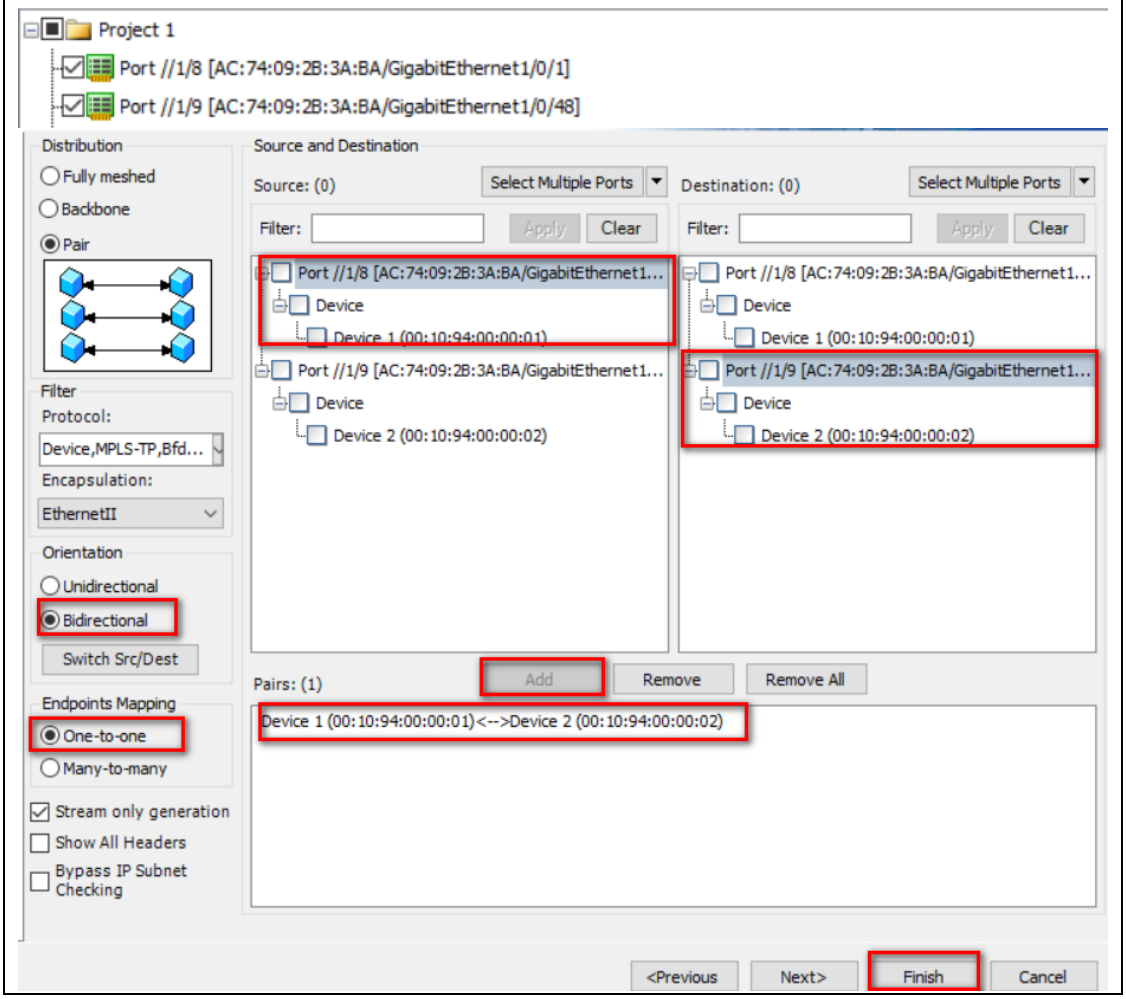
5. Add Devices under Port 1/8, Port 1/9, Port 4/5, Port 4/6, respectively

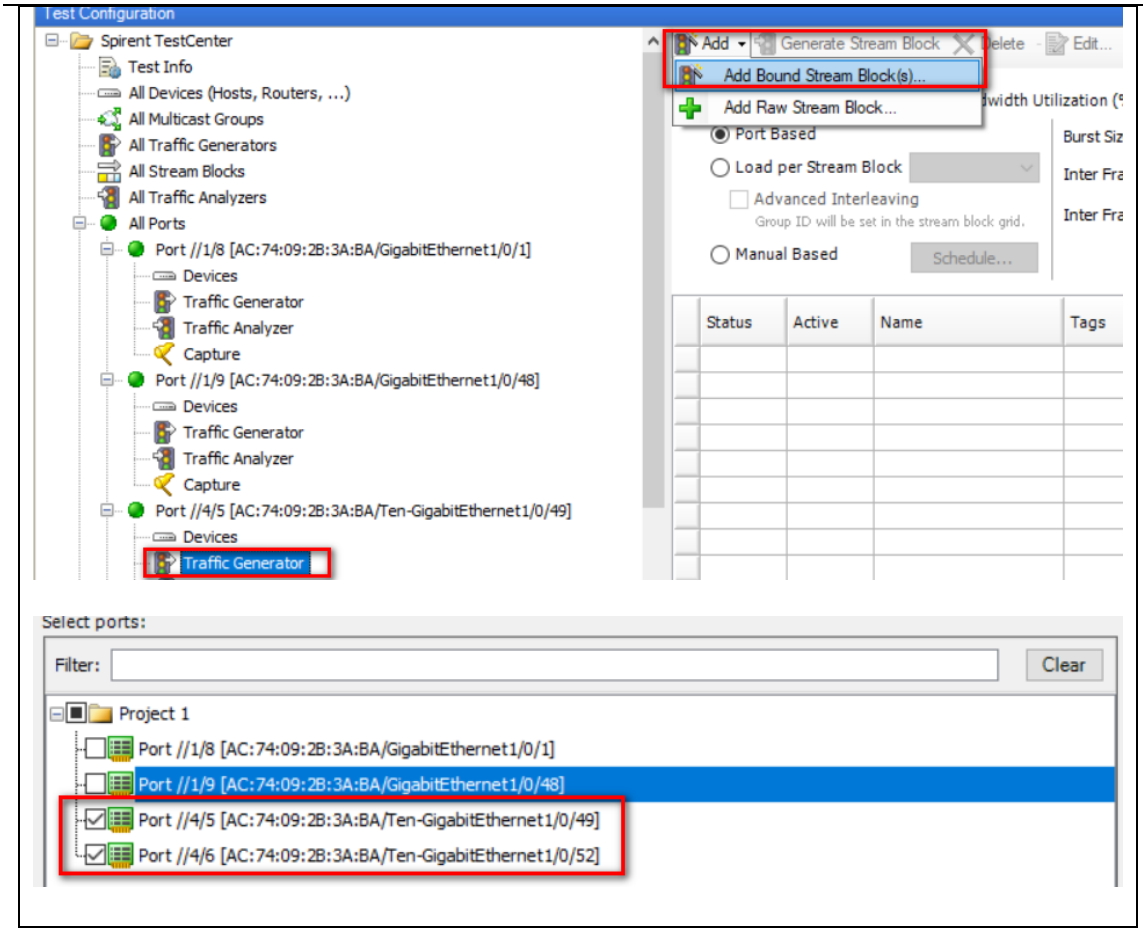


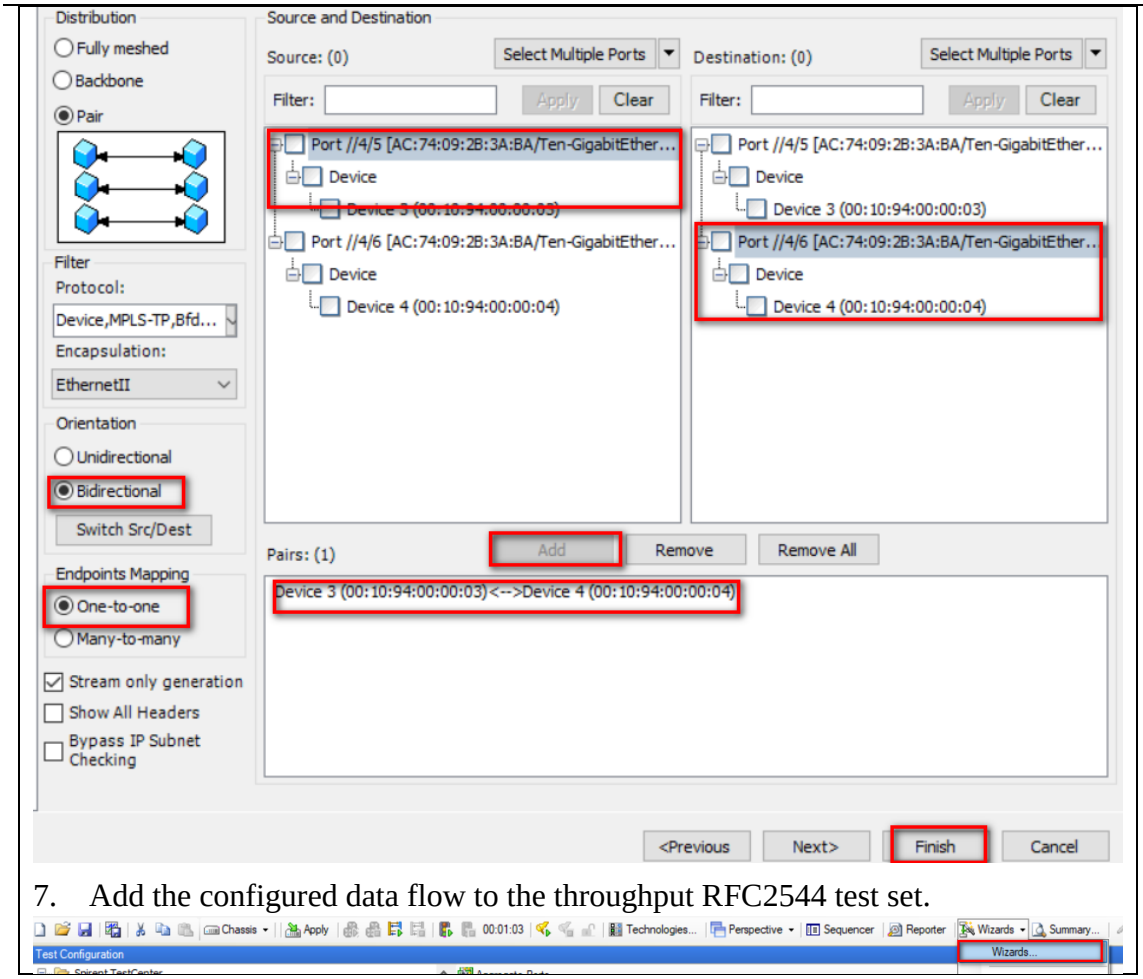


6. Add bound stream between Port 1/8 and Port 1/9, between Port 1/8, Port 1/9, respectively.

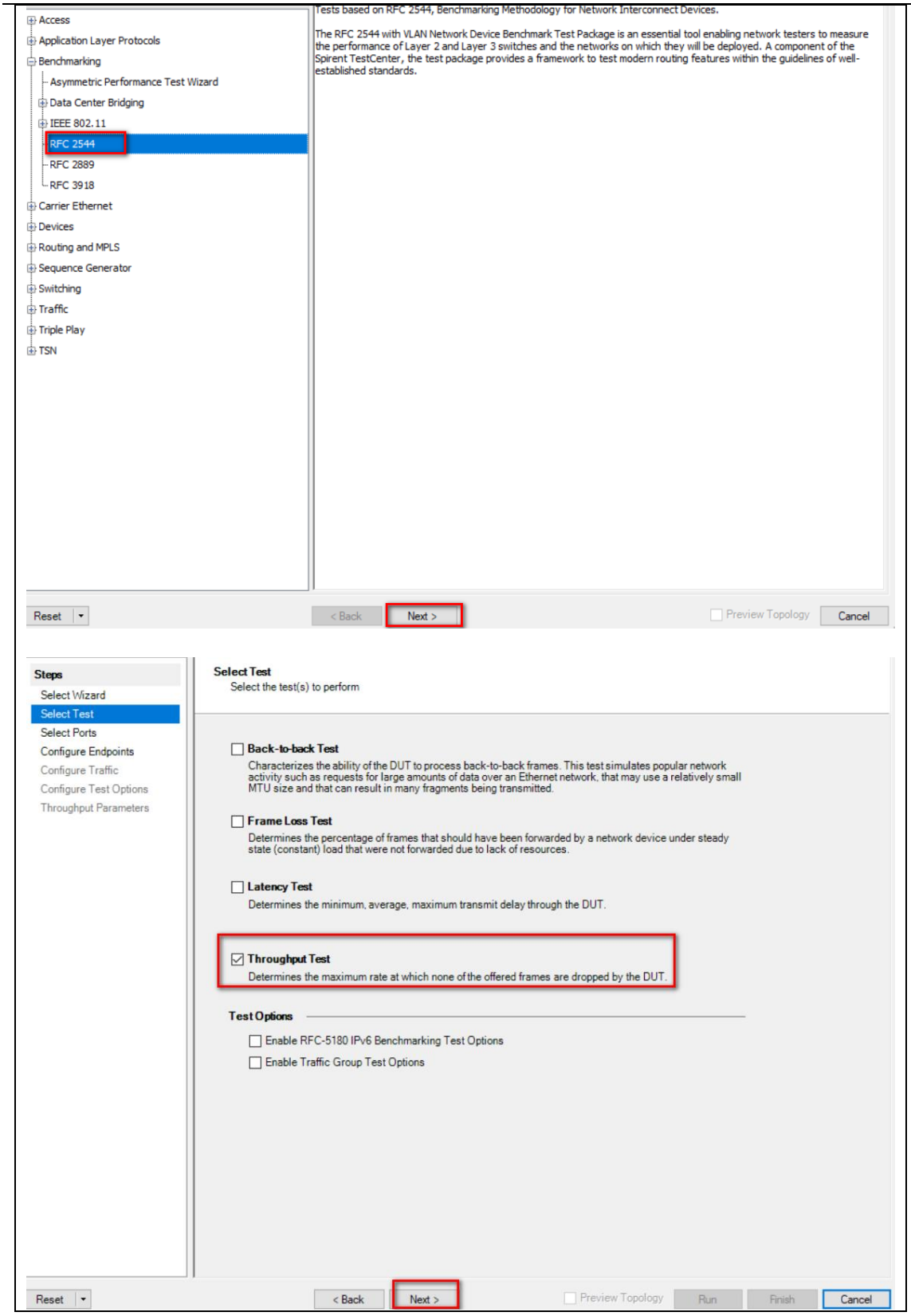


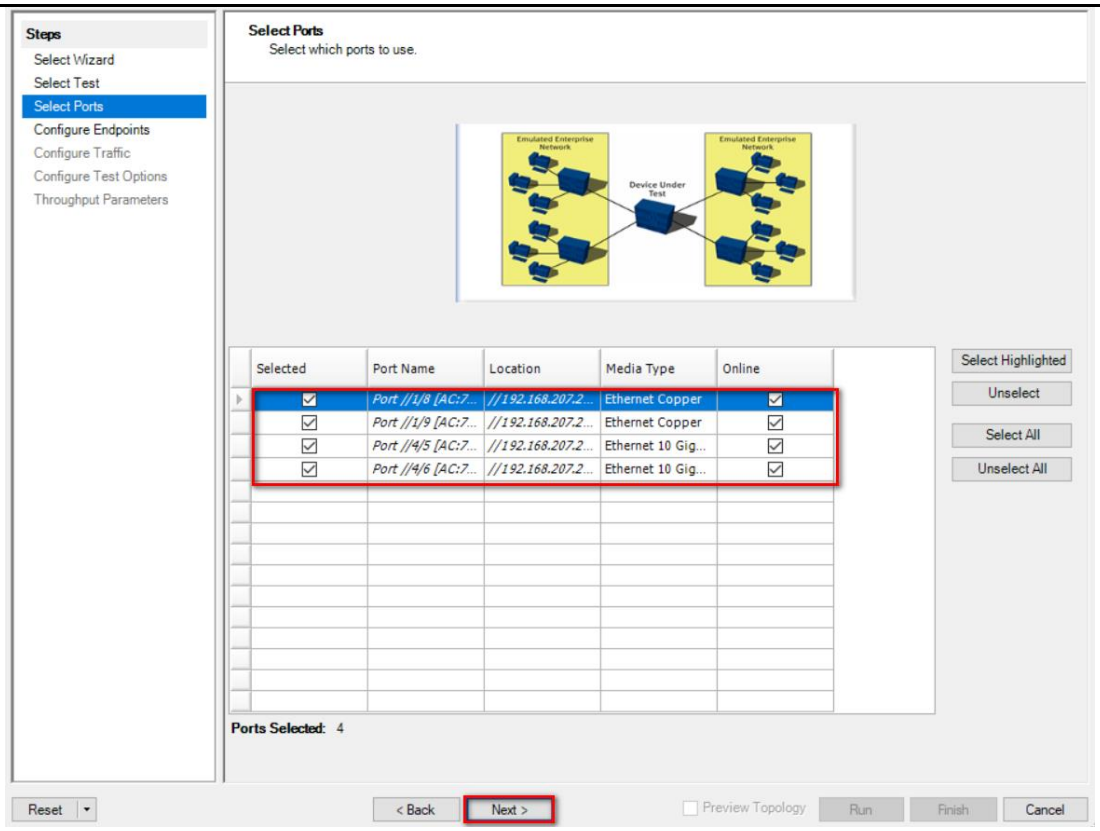


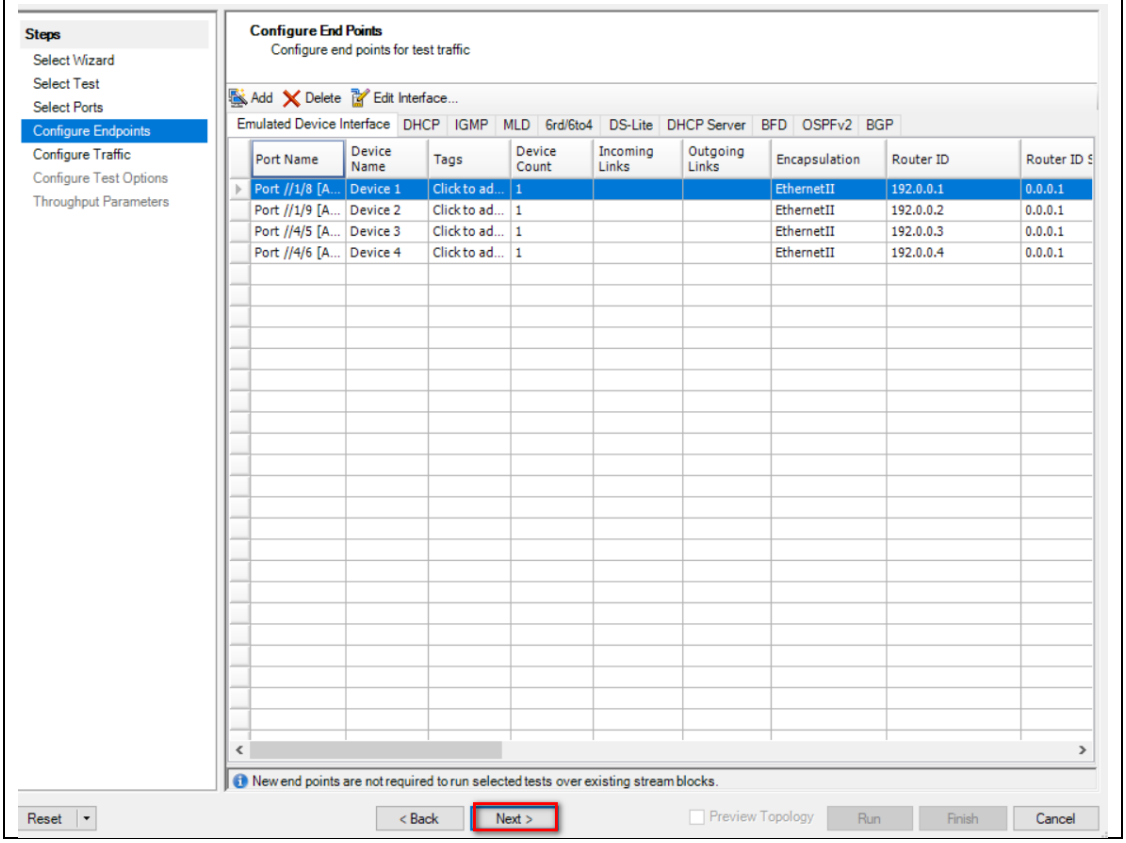


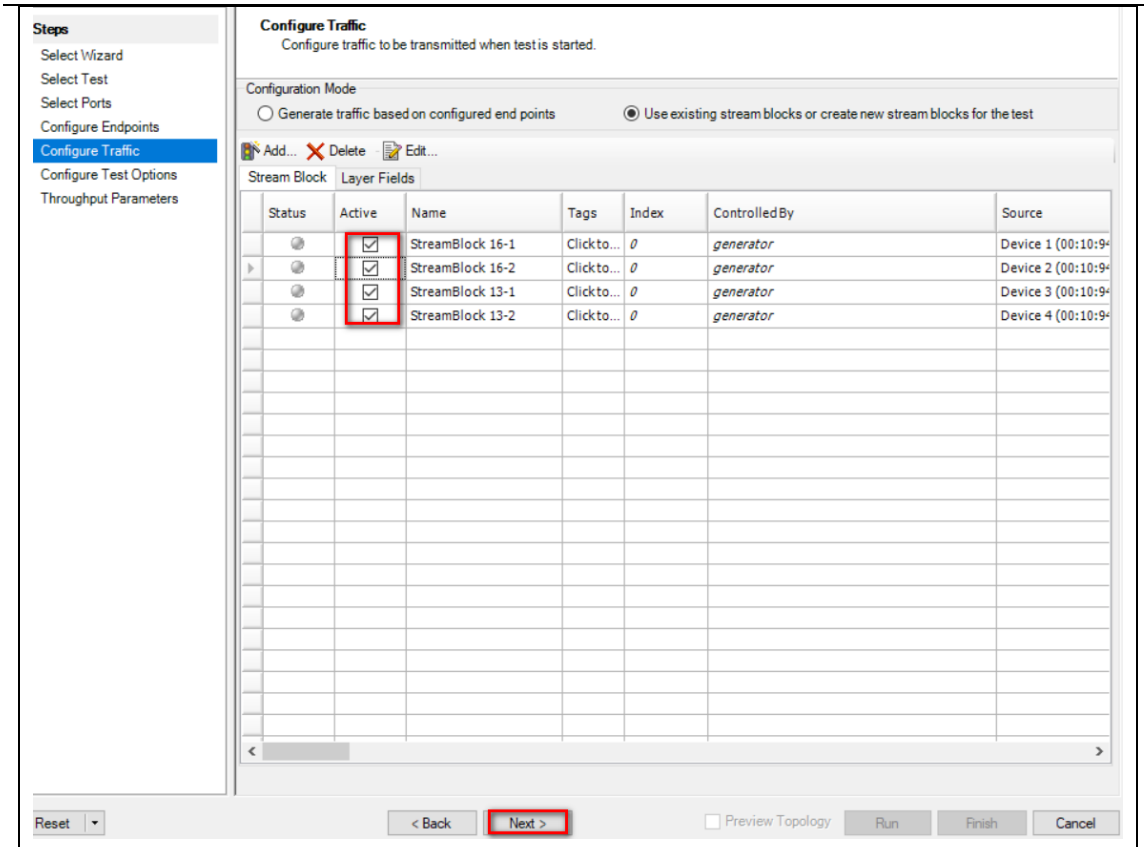


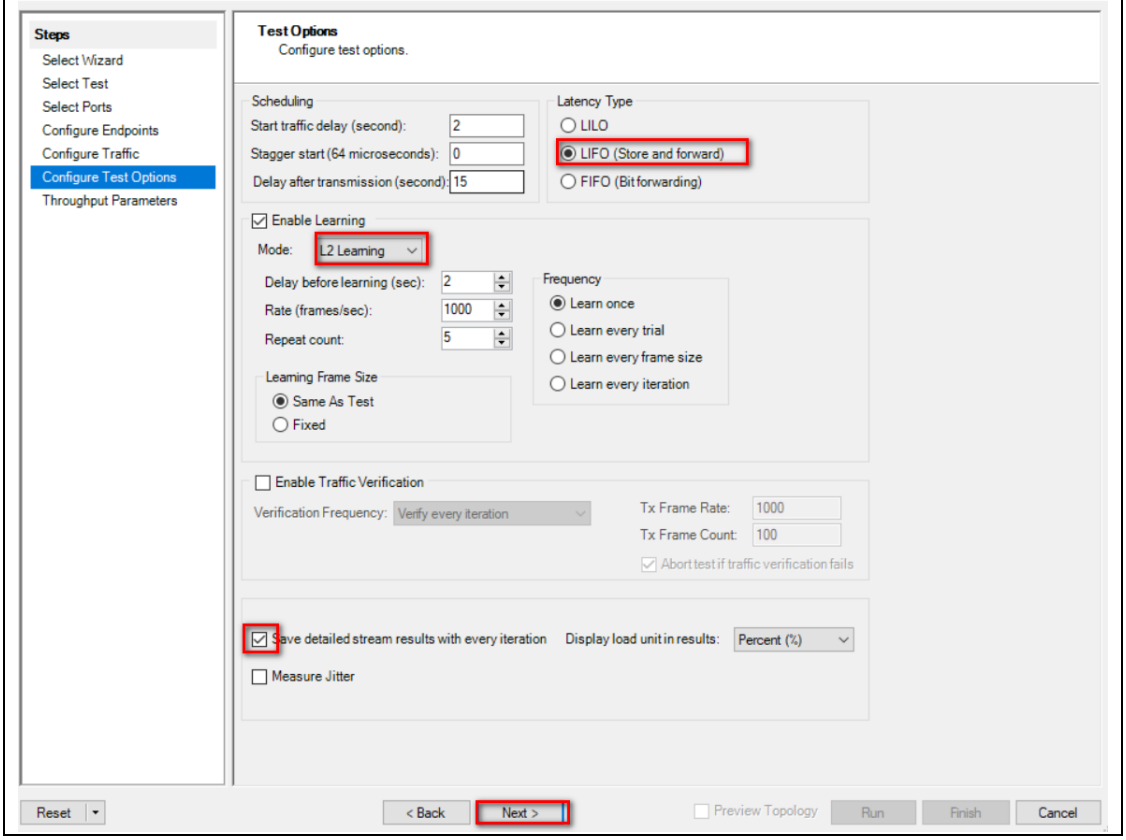
7. Add the configured data flow to the throughput RFC2544 test set.

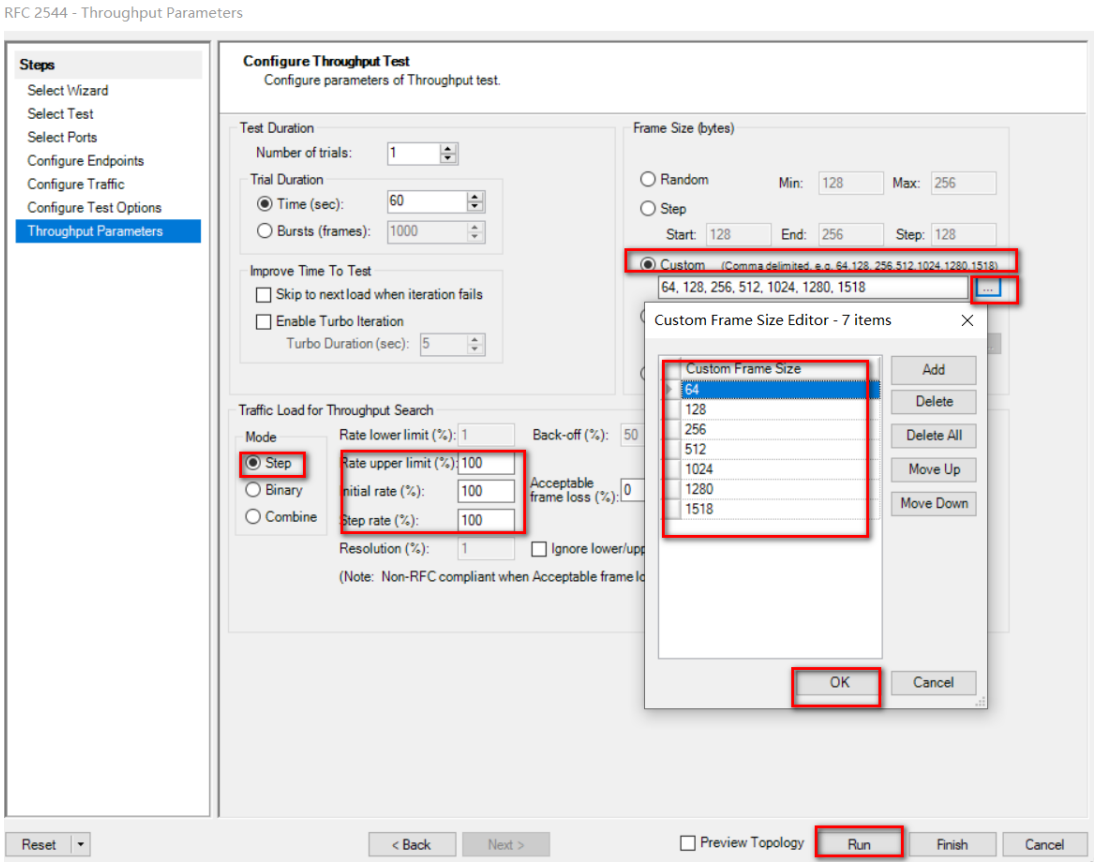




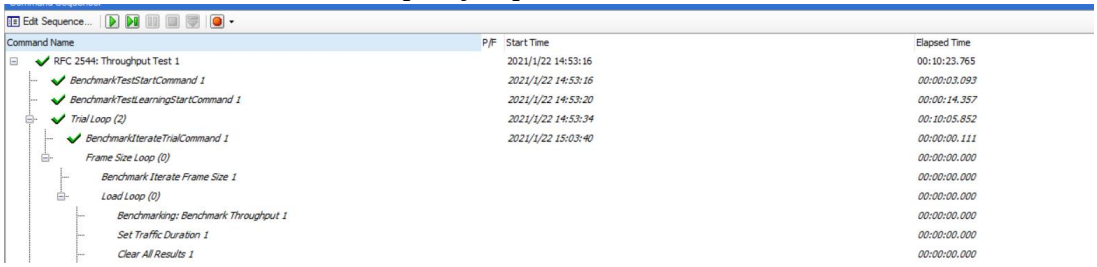








8. Then wait until this test report jump out.



9. Check the report, result1 is expected.

Trial Number	Id	Frame Size Type	Configured Frame Size	Avg Frame Size	iMIX Distribution	Intended Load (%)	Offered Load (%)	Result	Throughput (%)
1	0	Fixed	64	64	N/A	100	100	Passed	100
1	1	Fixed	128	128	N/A	100	100	Passed	100
1	2	Fixed	256	256	N/A	100	100	Passed	100
1	3	Fixed	512	512	N/A	100	100	Passed	100
1	4	Fixed	1,024	1,024	N/A	100	100	Passed	100
1	5	Fixed	1,280	1,280	N/A	100	100	Passed	100
1	6	Fixed	1,518	1,518	N/A	100	99.882	Passed	99.882

ad (%)	Offered Load (%)	Result	Throughput (%)	Max Latency Threshold Exceeded	Out Of Seq Threshold Exceeded	Tx Frame Count	Rx Frame Count	Frame Loss	Percent Loss	Offered Load (fps)	Forwarding Rate (fps)
	100	Passed	100	False	False	1,964,285,716	1,964,285,716	0	0	32,738,095.267	32,738,047.73
	100	Passed	100	False	False	1,114,864,866	1,114,864,866	0	0	18,581,081.1	18,581,044.94
	100	Passed	100	False	False	597,826,090	597,826,090	0	0	9,963,768.167	9,963,745.88
	100	Passed	100	False	False	310,150,378	310,150,378	0	0	5,169,172.967	5,169,156.1
	100	Passed	100	False	False	158,045,980	158,045,980	0	0	2,634,099.667	2,634,085.64
	100	Passed	100	False	False	126,923,078	126,923,078	0	0	2,115,384.633	2,115,372.42
	99.882	Passed	99.882	False	False	107,155,524	107,155,524	0	0	1,785,925.4	1,785,913.88

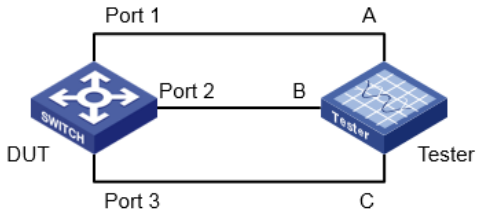
NOTE: scripts

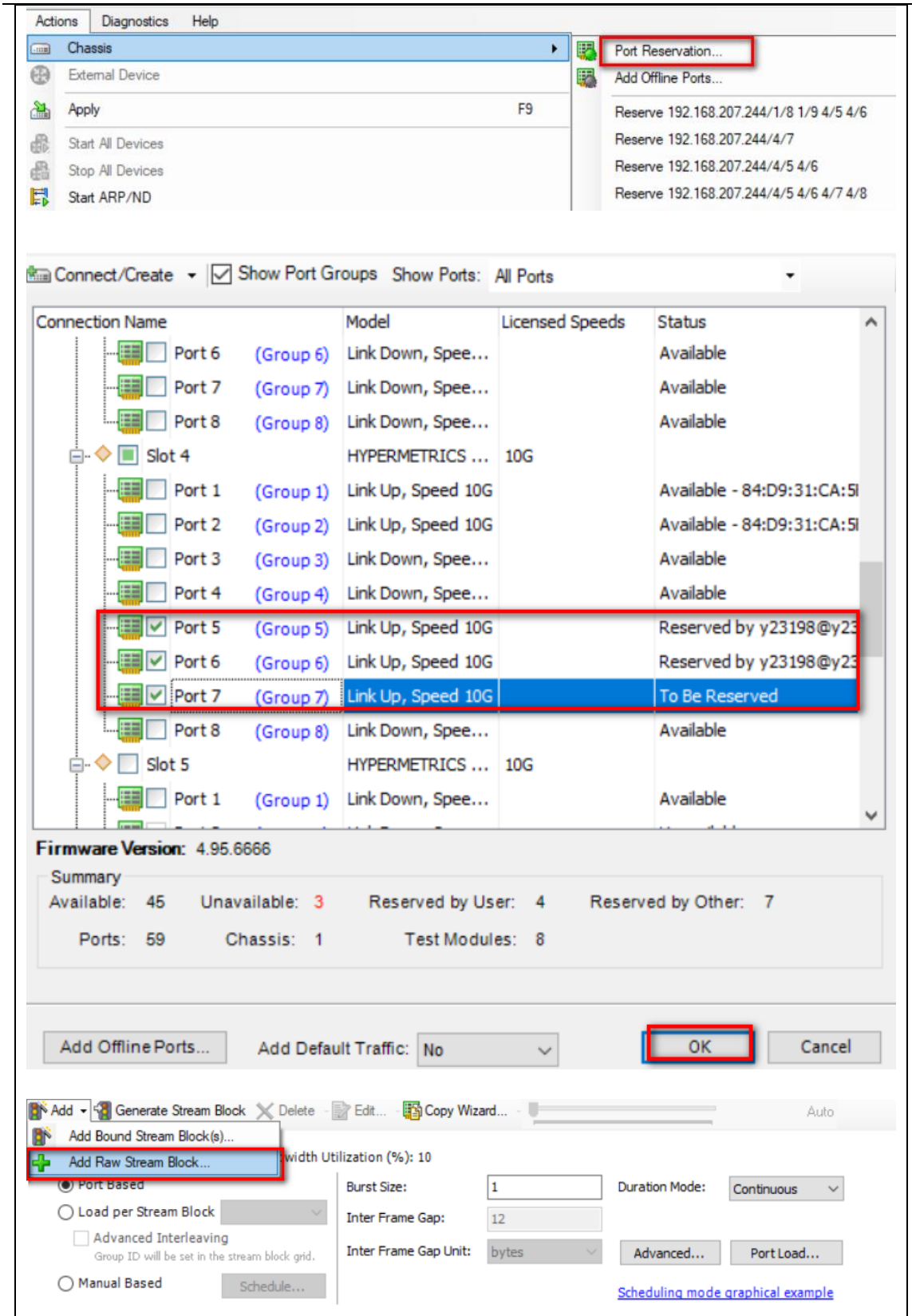
```
for {set i 2} {$i<=24} {incr i} {
    interface  GigabitEthernet1/0/[expr $i*2-1]
     port access vlan  [expr $i]
```

```
   interface  GigabitEthernet1/0/[expr $i*2]
    port access vlan [expr $i]
}

for {set i 25} {$i<=26} {incr i} {
    interface  Ten-GigabitEthernet  1/0/[expr $i*2-1]
     port access vlan  [expr $i]
    interface  Ten-GigabitEthernet  1/0/[expr $i*2]
     port access vlan [expr $i]
}
```

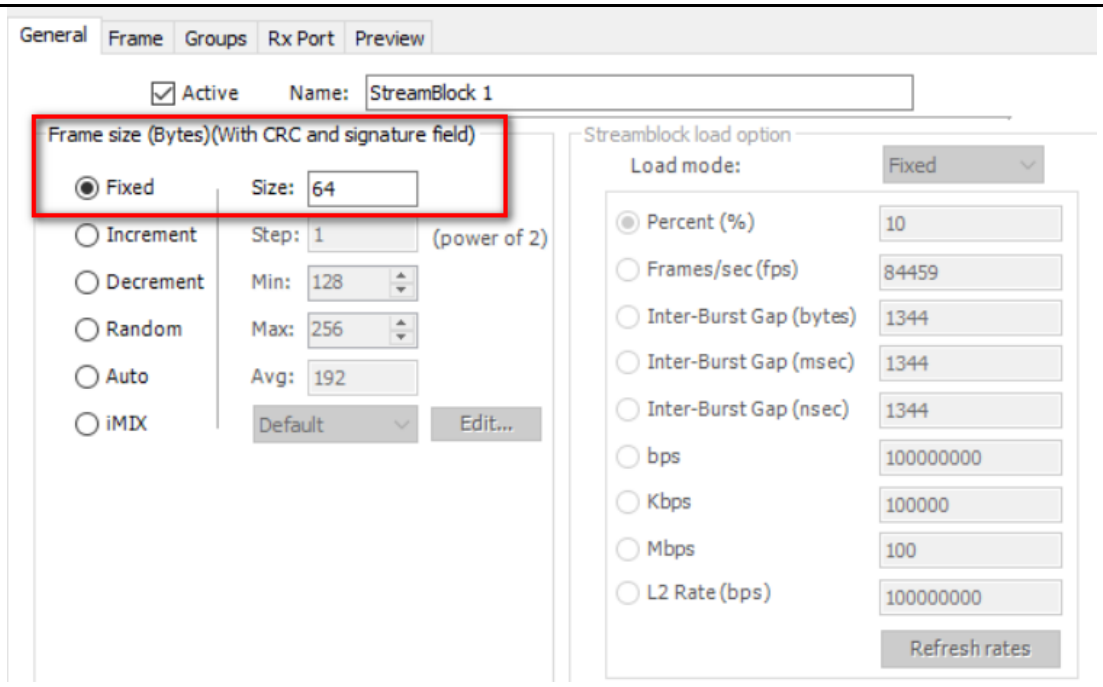
☐ Passed	☐ Failed

1.2 MAC address table capacity

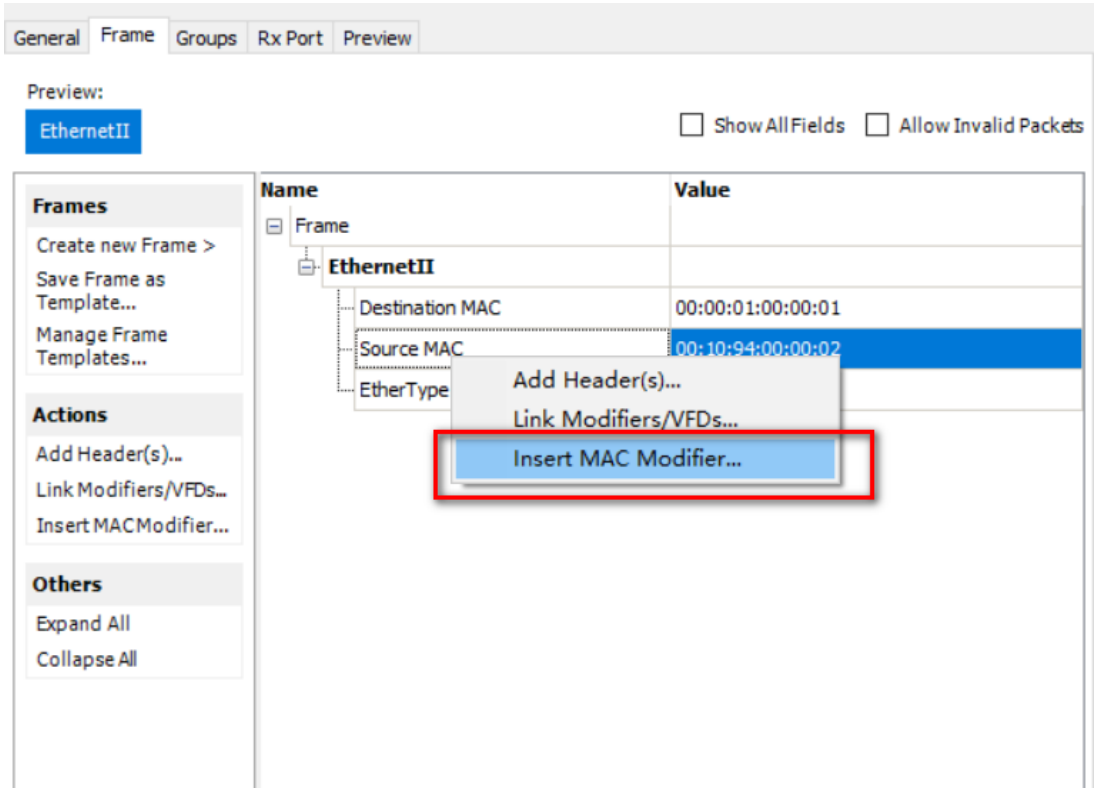
Test Item Name: MAC address table capacity
Work Hour: 30 min
Test Topology: 
Test Process: 1. On the tester, send broadcast packets through Port A. The source MAC addresses of the packets are 16K consecutive MAC addresses. 2. On the tester, send unicast packets through Port B. The destination MAC addresses are the MAC addresses that the DUT has learned. Result 1 is expected.
Expect Results: 1. On the tester, Port B receives all the packets sent by Port B. If traffic loss occurs, the MAC address table capacity does not meet the 16K specification.
Actual Result： 1. Select the “Traffic Generator” under PORT A, and click “Add Raw Stream Block...” in the context menu of the interface



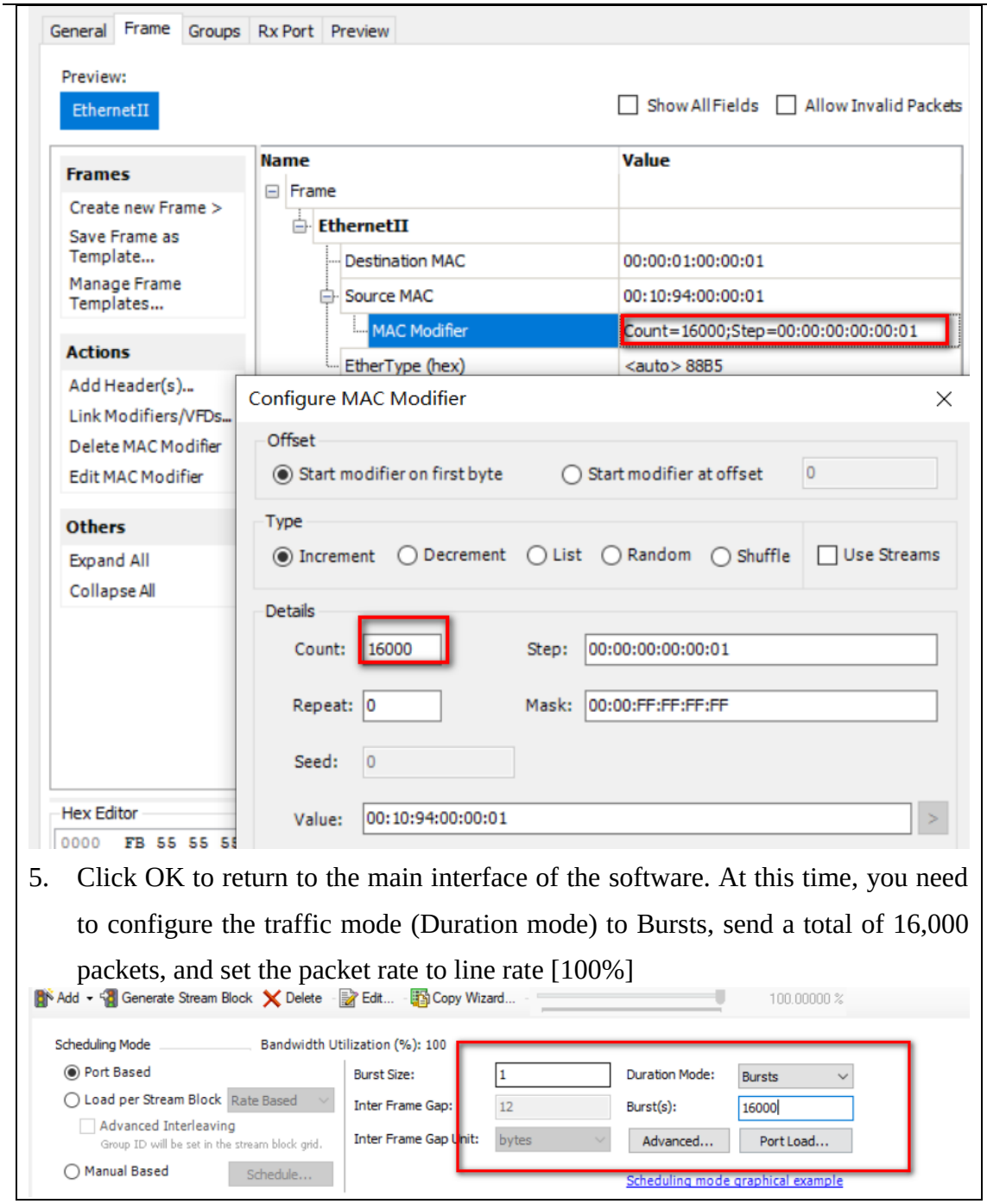
2. First configure the packet size in the General tab, set to 64Bytes



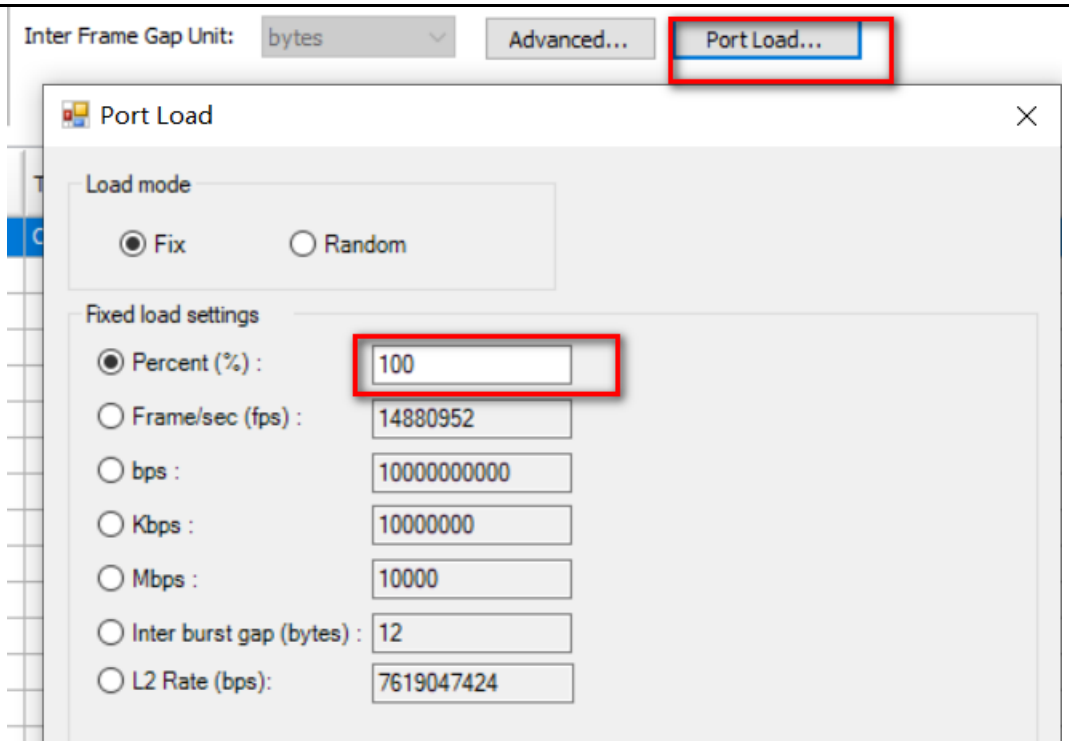
3. Right-click on the “Source MAC “field in the Frame tab and select “Insert MAC Modifier...” from the menu



4. Construct 16K packets with different MAC addresses on the PORT A of the tester to fill the DUT's MAC address table



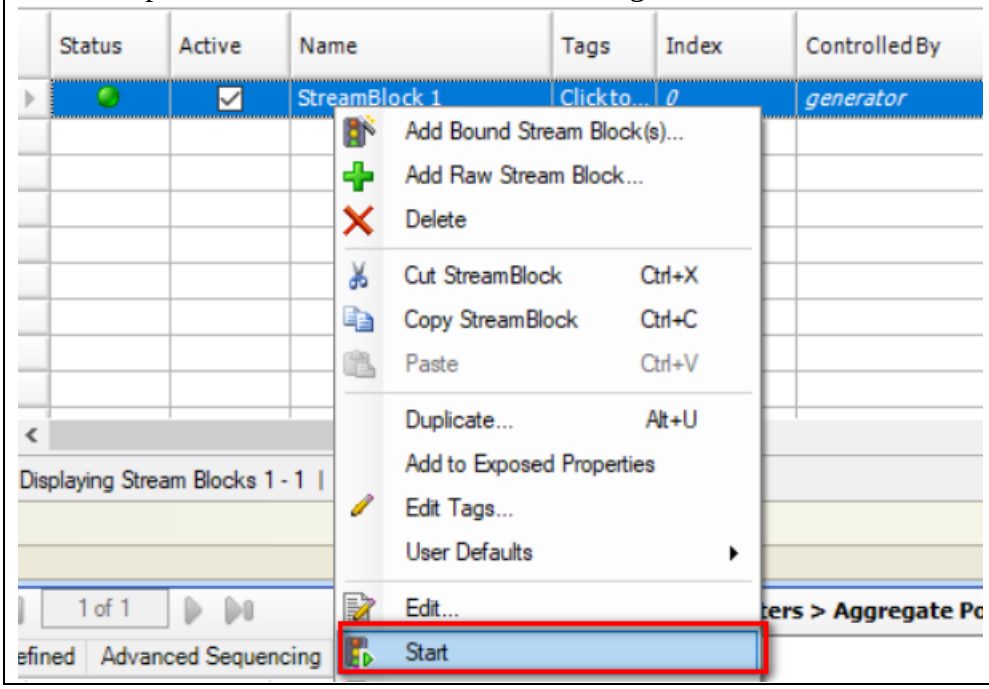
5. Click OK to return to the main interface of the software. At this time, you need to configure the traffic mode (Duration mode) to Bursts, send a total of 16,000 packets, and set the packet rate to line rate [100%]



6. Before sending traffic, clear the MAC address on the DUT and verify that the number of MAC addresses on the DUT is 0

```
[DUT]undo mac-address
This will delete all non-MacAuth entries. Continue? [Y/N]:y
[DUT]display mac-address count
0 mac address(es) found.
```

7. Send packet.You can see that in the resulting view, PORT A sent 40,000 packets.

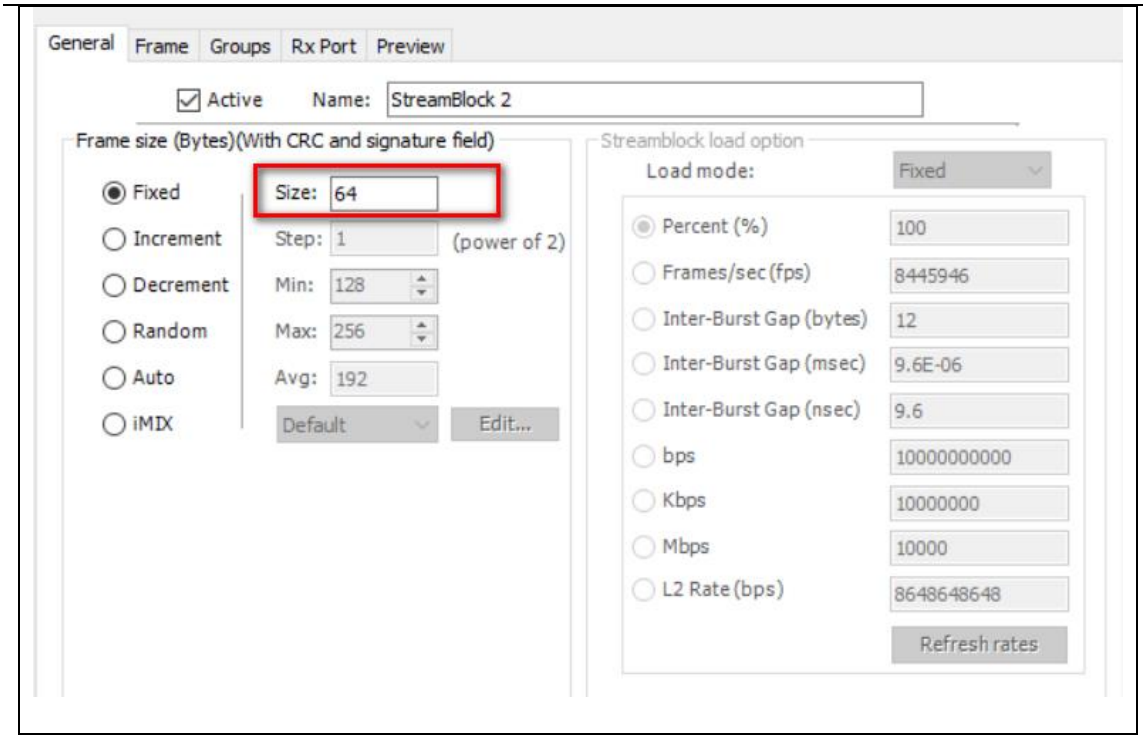


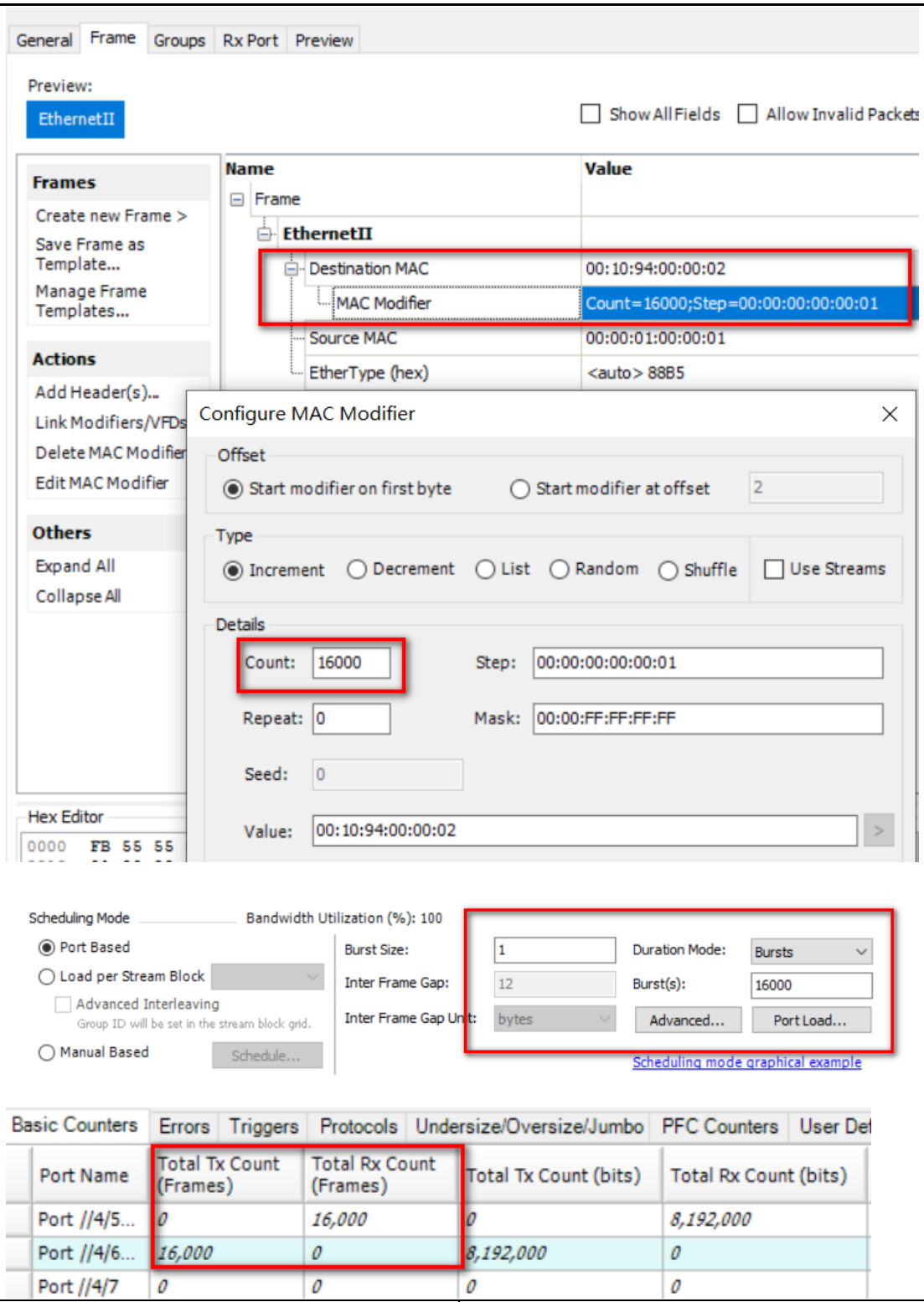
Port Name	Total Tx Count (Frames)	Total Rx Count (Frames)	Total Tx Count (bits)	Total Rx Count (bits)
Port //4/5...	16,000	0	8,192,000	0
Port //4/6...	0	16,000	0	8,192,000
Port //4/7	0	16,000	0	8,192,000

8. At this time, check the number of MAC addresses on the DUT.

```
[DUT]display mac-address
MAC Address      VLAN ID    State           Port/Nickname           Aging
0010-9400-0002   1          Learned         XGE1/0/49               Y
0010-9400-0003   1          Learned         XGE1/0/49               Y
0010-9400-0004   1          Learned         XGE1/0/49               Y
0010-9400-0005   1          Learned         XGE1/0/49               Y
0010-9400-0006   1          Learned         XGE1/0/49               Y
0010-9400-0007   1          Learned         XGE1/0/49               Y
0010-9400-0008   1          Learned         XGE1/0/49               Y
0010-9400-0009   1          Learned         XGE1/0/49               Y
0010-9400-000a   1          Learned         XGE1/0/49               Y
0010-9400-000b   1          Learned         XGE1/0/49               Y
0010-9400-000c   1          Learned         XGE1/0/49               Y
0010-9400-000d   1          Learned         XGE1/0/49               Y
0010-9400-000e   1          Learned         XGE1/0/49               Y
0010-9400-000f   1          Learned         XGE1/0/49               Y
0010-9400-0010   1          Learned         XGE1/0/49               Y
0010-9400-0011   1          Learned         XGE1/0/49               Y
0010-9400-0012   1          Learned         XGE1/0/49               Y
0010-9400-0013   1          Learned         XGE1/0/49               Y
0010-9400-0014   1          Learned         XGE1/0/49               Y
0010-9400-0015   1          Learned         XGE1/0/49               Y
0010-9400-0016   1          Learned         XGE1/0/49               Y
0010-9400-0017   1          Learned         XGE1/0/49               Y
[DUT]display mac-address count
16000 mac address(es) found.
```

9. The traffic is sent from PORT B. The destination MAC address is the source MAC address configured on PORT A in the above step, to verify that the learned MAC address can work normally, because all the destination mac address belong to Port A , Port C can’t receive the traffic and result 1 is expected





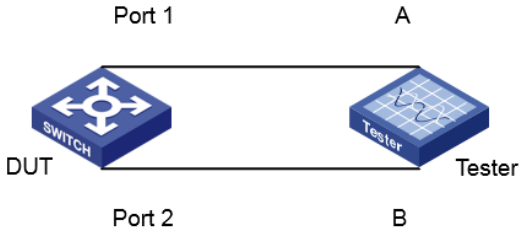
☐ Passed	☐ Failed

1.3 Multicast Group Capacity

Test Item Name: Multicast Group Capacity

Work Hour: 20 min

Test Topology:



Test Process:

1. Create VLAN 100, assign Port A/B of DUT to join VLAN 100.
2. Enable igmp-snooping globally, enable igmp-snooping enable within VLAN 100.
3. The DUT Port B is configured with igmp-snooping static-group 225.0.0.1 vlan 100, and the IP address is increased by 0.0.0.1 to a total of 1000 multicast groups.
4. DUT display igmp-snooping static-group, result 1 is expected.
5. Send the destination IP 225.0.0.1 into port A of tester, change the multicast traffic of 1000 groups in total, check the packet of Port B of tester, result 2 is expected.

Expect Results:

1. DUT display igmp-snooping static-group has 1000 correct static groups.
2. The Tester Port B can receive the traffic of 1000 multicast groups starting from 225.0.0.1.

Actual Result:

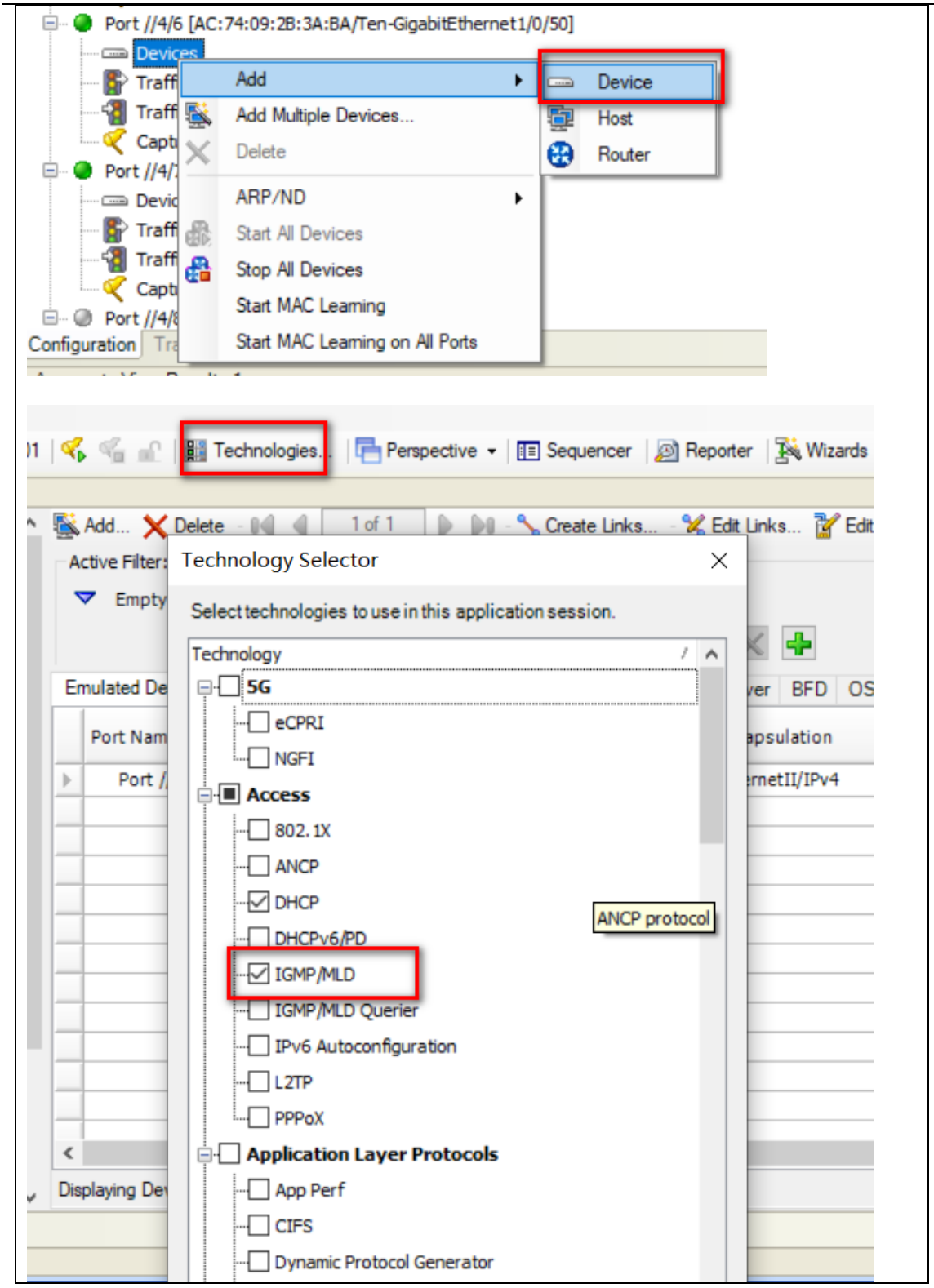
1. Create VLAN 100, assign Port A/B of DUT to join VLAN 100

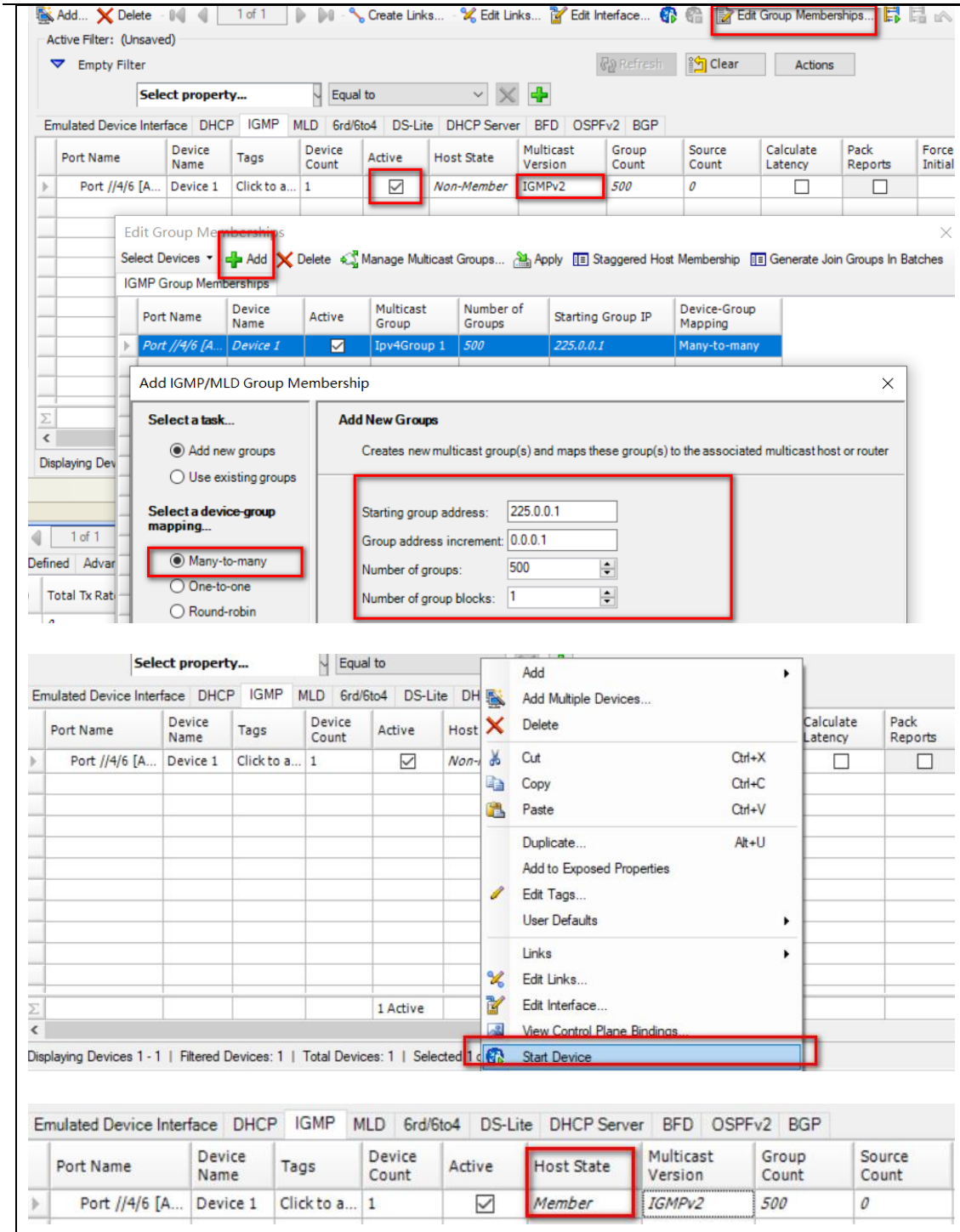
```
[DUT-vlan100]port Ten-GigabitEthernet 1/0/49
[DUT-vlan100]port Ten-GigabitEthernet 1/0/50
```

2. Enable igmp-snooping globally, enable igmp-snooping enable within VLAN 100

```
[DUT]igmp-snooping
[DUT-igmp-snooping]quit
[DUT]vlan 100
[DUT-vlan100]igmp-snooping enable
```

3. The DUT Port B is configured with igmp-snooping static-group 225.0.0.1 vlan 100, and the IP address is increased by 0.0.0.1 to a total of 1000 multicast groups

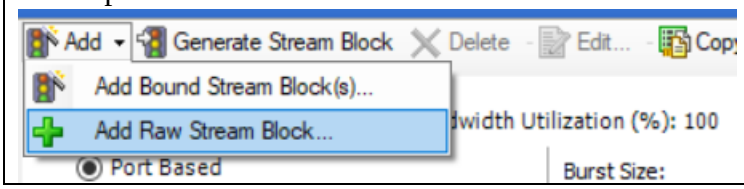


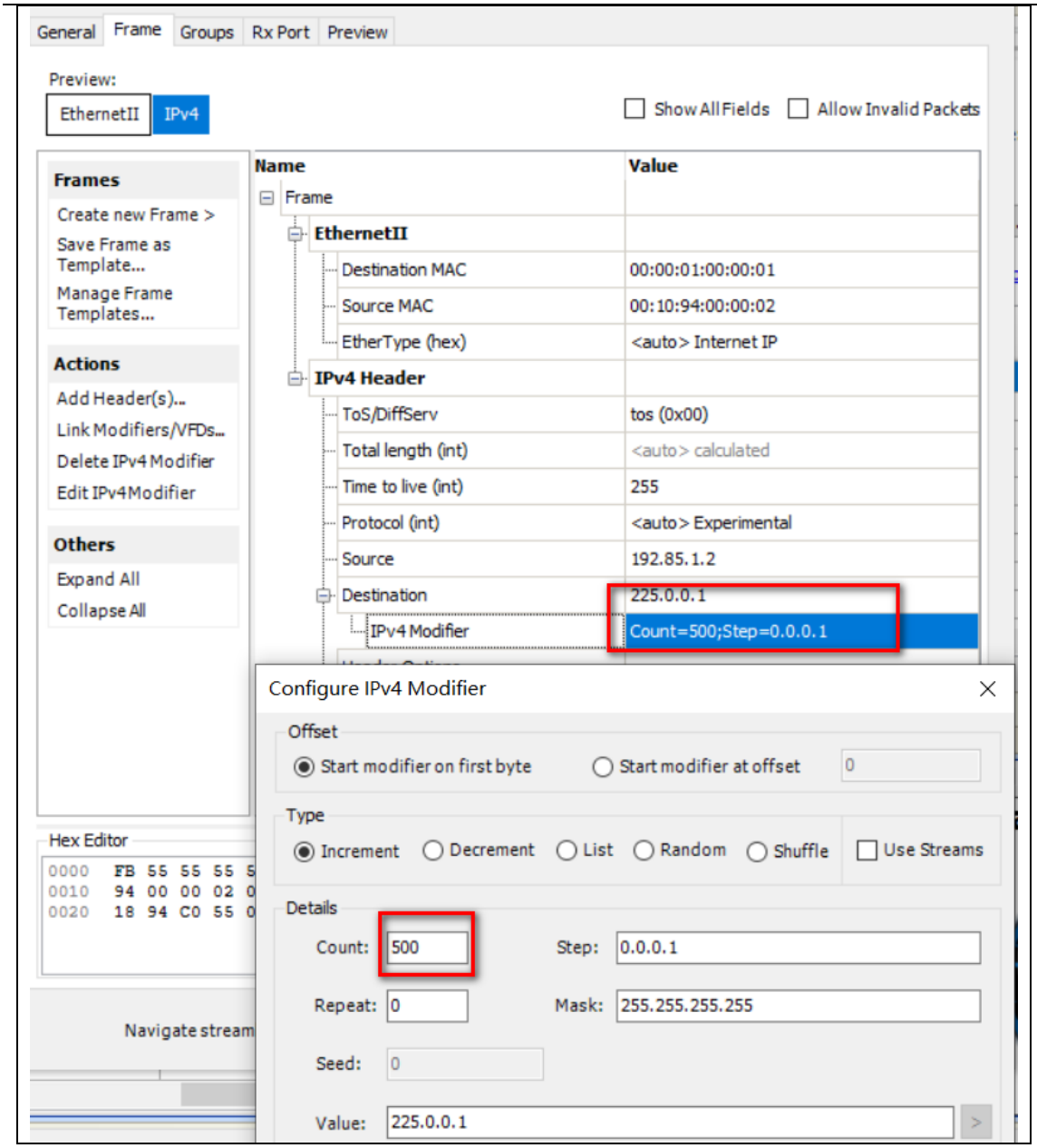


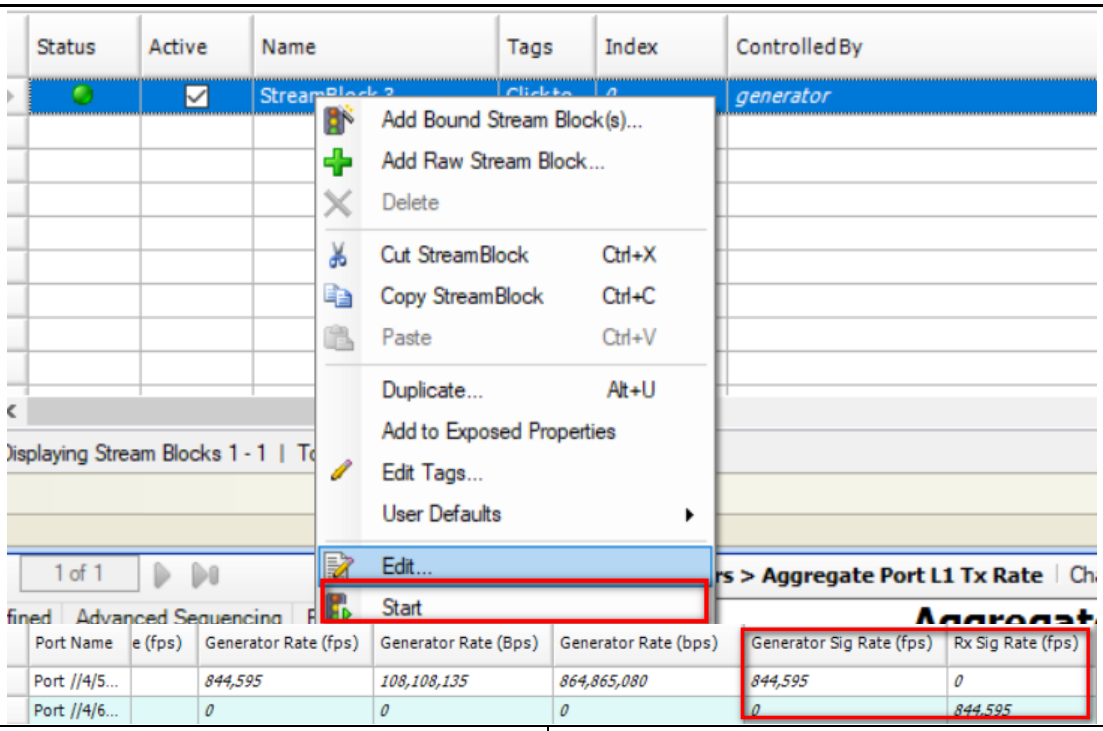
4. DUT display igmp-snooping static-group, result 1 is expected

```
[DUT-vlan100]dis igmp-snooping group
Total 500 entries.

VLAN 100: Total 500 entries.
  (0.0.0.0, 225.0.0.1)
    Host ports (1 in total):
      XGE1/0/50                                (00:04:11)
  (0.0.0.0, 225.0.0.2)
    Host ports (1 in total):
      XGE1/0/50                                (00:04:16)
  (0.0.0.0, 225.0.0.3)
    Host ports (1 in total):
      XGE1/0/50                                (00:04:13)
  (0.0.0.0, 225.0.0.4)
    Host ports (1 in total):
      XGE1/0/50                                (00:04:16)
  (0.0.0.0, 225.0.0.5)
    Host ports (1 in total):
      XGE1/0/50                                (00:04:15)
  (0.0.0.0, 225.0.0.6)
    Host ports (1 in total):
      XGE1/0/50                                (00:04:16)
  (0.0.0.0, 225.0.0.7)
    Host ports (1 in total):
---- More ----
```

5. 5. Send the destination IP 225.0.0.1 into port A of tester, change the multicast traffic of 1000 groups in total, check the packet of Port B of tester, result 2 is expected







☐ Passed	☐ Failed

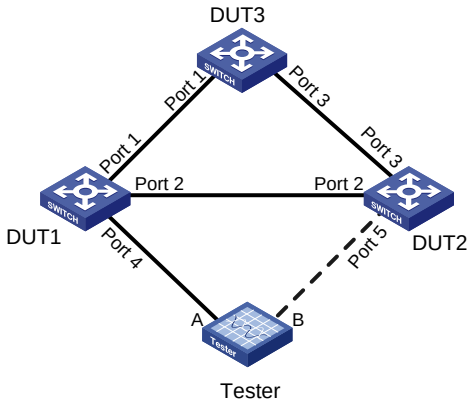
2 Layer 2 protocol

2.1 STP

Test Item Name: STP

Work Hour: 30 min

Test Topology:



Test Process:

1. On the DUTs, set the spanning tree mode to STP and execute the STP global mcheck command.
2. Configure DUT 1 as the root bridge.
3. View the STP status on the DUTs. On the tester, send broadcast traffic through Port A for 1 minute. Result 1 is expected.
4. On the tester, construct Layer 2 unicast packets and the reversed packets (source and destination MAC addresses are swapped). Send all the packets continuously through Port A and Port B. Result 2 is expected.
5. Remove the link between DUT 1 and DUT 2. Result 3 is expected.
6. Reconnect DUT 1 to DUT 2. Result 3 is expected.

Expect Results:

1. DUTs can calculate spanning trees correctly.
2. DUTs can recalculate spanning trees correctly in 30 seconds.

Actual Result：

1. Enable STP globally

[DUT] stp global enable

[DUT] stp mode stp

2. Configure DUT1 as the root bridge

[DUT1] stp root primary

3. Check the STP status on DUT

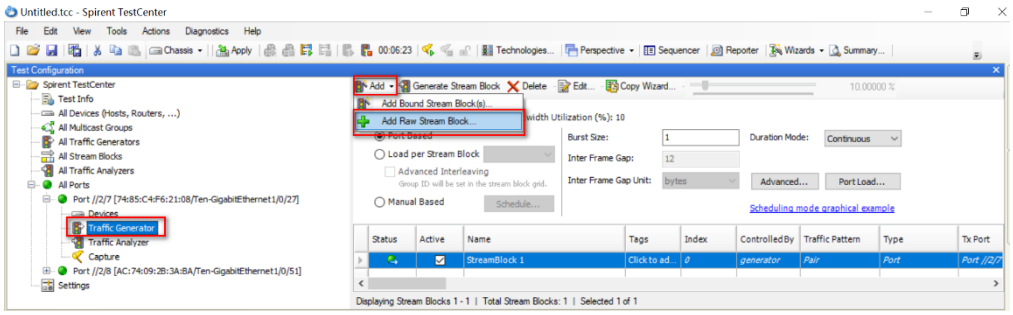
Display stp brief

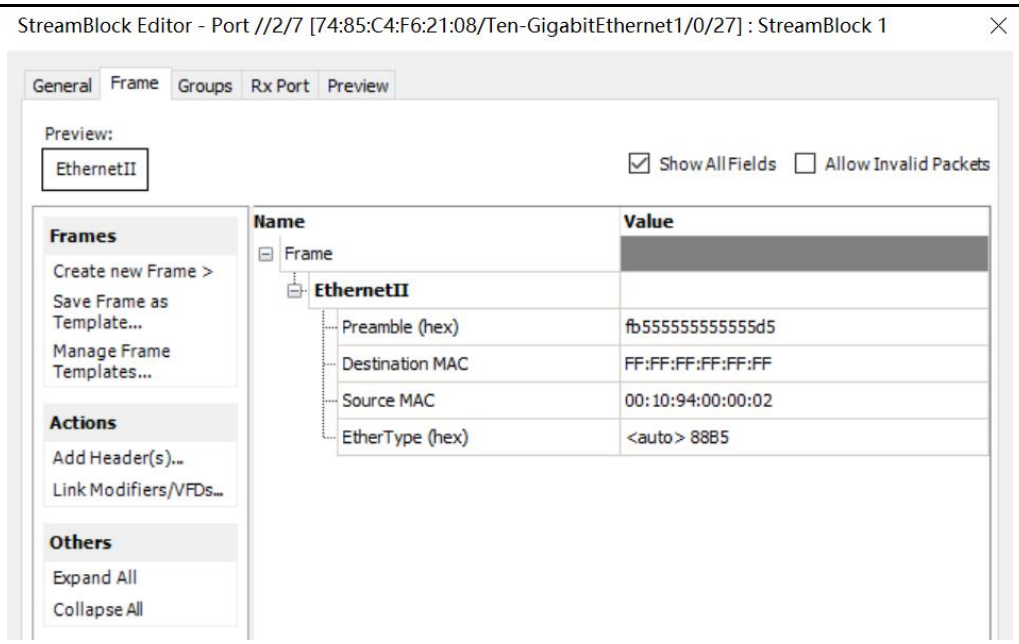
```
[DUT1]dis stp br
 MST ID   Port                                    Role  STP State     Protection
 0        Ten-GigabitEthernet1/0/25               DESI  FORWARDING    NONE
 0        Ten-GigabitEthernet1/0/26               DESI  FORWARDING    NONE
 0        Ten-GigabitEthernet1/0/27               DESI  FORWARDING    NONE
[DUT1]
```

```
[DUT2]dis stp br
 MST ID   Port                                    Role  STP State     Protection
 0        Ten-GigabitEthernet1/0/49               ROOT  FORWARDING    NONE
 0        Ten-GigabitEthernet1/0/50               ALTE  DISCARDING    NONE
 0        Ten-GigabitEthernet1/0/51               DESI  FORWARDING    NONE
[DUT2]
```

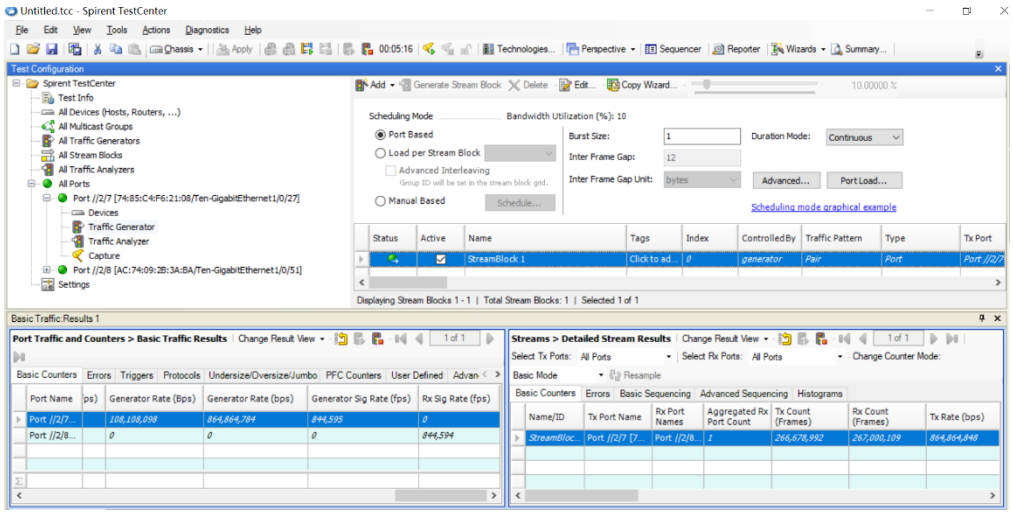
```
[DUT3]dis stp br
 MST ID   Port                                    Role  STP State     Protection
 0        Ten-GigabitEthernet1/0/24               ROOT  FORWARDING    NONE
 0        Ten-GigabitEthernet1/0/39               DESI  FORWARDING    NONE
[DUT3]
```

4. Send broadcast traffic on Port A





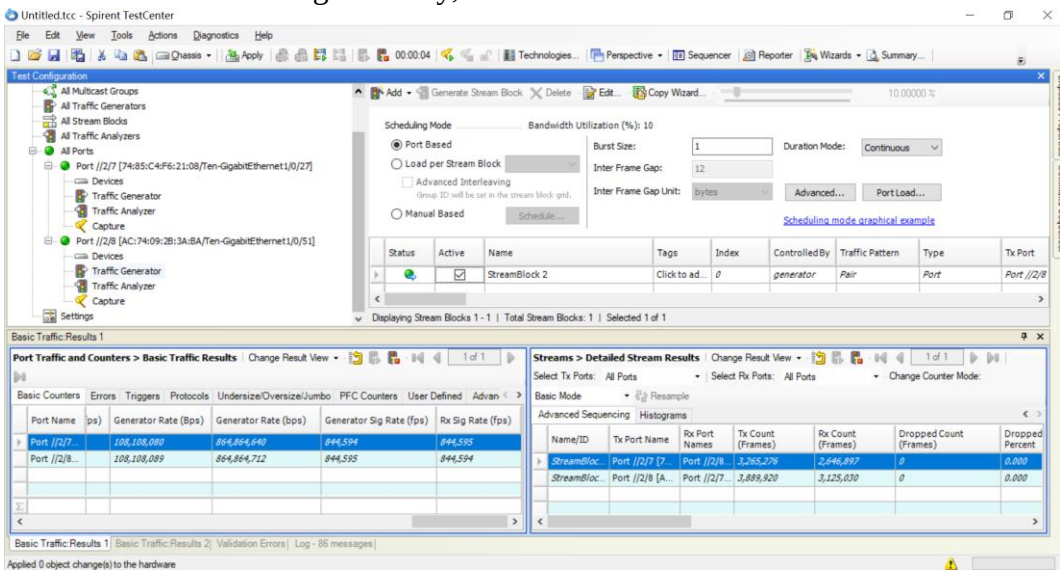
5. No broadcast storm occurs.




```
[DUT1]d c r  i i
Usage: Bandwidth utilization in percentage
Interface            Usage (%)    Total (pps)    Broadcast (pps)    Multicast (pps)
XGE1/0/25                    0              0                 --                 --
XGE1/0/26                    0              0                 --                 --
XGE1/0/27                   10         844575                 --                 --

 Overflow: More than 14 digits.
       --: Not supported.
[DUT1]d c r o i
Usage: Bandwidth utilization in percentage
Interface            Usage (%)    Total (pps)    Broadcast (pps)    Multicast (pps)
XGE1/0/25                   10         844575                 --                 --
XGE1/0/26                   10         844575                 --                 --
XGE1/0/27                    0              0                 --                 --

 Overflow: More than 14 digits.
       --: Not supported.
```

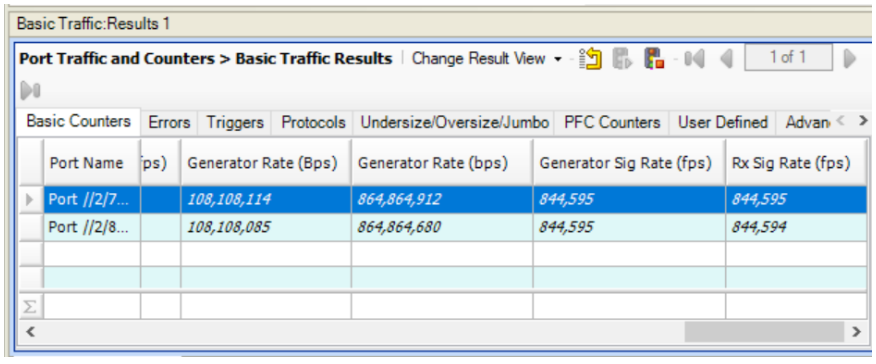
6. Send bi-direction unicast traffic

7. Traffic is forwarding normally, and no traffic loss occurs



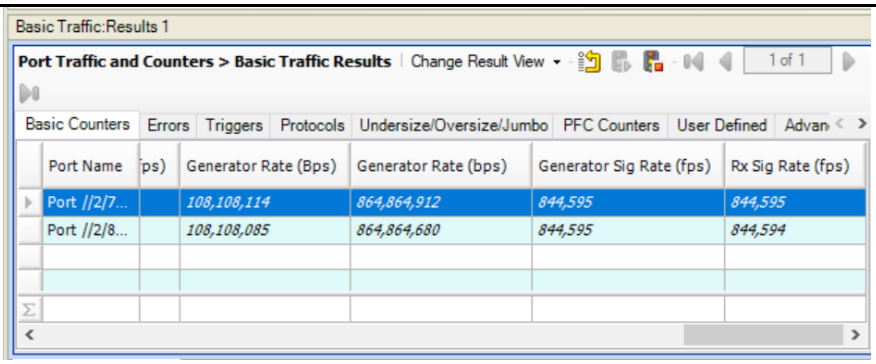
8. Remove the link between DUT 1 and DUT 2 and traffic can recover within 30s

```
[DUT1-Ten-GigabitEthernet1/0/25]shu
%Jan 28 10:26:57:762 2021 DUT1 STP/6/STP_NOTIFIED_TC: Instance 0's port Ten-GigabitEthernet1/0/2
6 was notified a topology change.
%Jan 28 10:26:57:777 2021 DUT1 IFNET/3/PHY_UPDOWN: Physical state on the interface Ten-GigabitEt
hernet1/0/25 changed to down.
%Jan 28 10:26:57:868 2021 DUT1 IFNET/5/LINK_UPDOWN: Line protocol state on the interface Ten-Gig
abitEthernet1/0/25 changed to down.
[DUT1-Ten-GigabitEthernet1/0/25]
```



9. Reconnect DUT 1 to DUT 2 and traffic can recover within 30s

```
[DUT1-Ten-GigabitEthernet1/0/25]und shu
[DUT1-Ten-GigabitEthernet1/0/25]%Jan 28 10:47:39:157 2021 DUT1 IFNET/3/PHY_UPDOWN: Physical stat
e on the interface Ten-GigabitEthernet1/0/25 changed to up.
%Jan 28 10:47:39:161 2021 DUT1 IFNET/5/LINK_UPDOWN: Line protocol state on the interface Ten-Gig
abitEthernet1/0/25 changed to up.
```



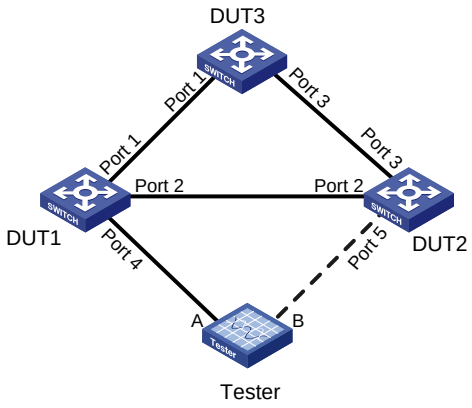
☐ Passed	☐ Failed

2.2 RSTP

Test Item Name: RSTP

Work Hour: 40 min

Test Topology:



Test Process:

1. On the DUTs, set the spanning tree mode to RSTP
2. Configure DUT 1 as the root bridge.
3. View the RSTP status on the DUTs. On the tester, send broadcast traffic through Port A for 1 minute. Result 1 is expected.
4. On the tester, construct Layer 2 unicast packets and the reversed packets (source and destination MAC addresses are swapped). Send all the packets continuously through Port A and Port B. Result 2 is expected.
5. Configure Port 4 of DUT 1 and Port 5 of DUT 2 as edge ports.

6. Remove the link between DUT 1 and DUT 2. Result 3 is expected.
7. Reconnect DUT 1 to DUT 2. Result 3 is expected.
8. Modify the spanning tree parameters of the DUTs and verify whether the DUTs can recalculate spanning trees based on the modifications. Result 3 is expected.

Expect Results:

1. DUTs can calculate spanning trees correctly.
2. DUTs can recalculate spanning trees correctly within 2s.

Actual Results:

1. Set STP mode to RSTP on DUT

[DUT] stp global enable

[DUT] stp mode rstp

2. Configure DUT1 as root bridge

[DUT1] stp root primary

3. Check the STP status on DUT

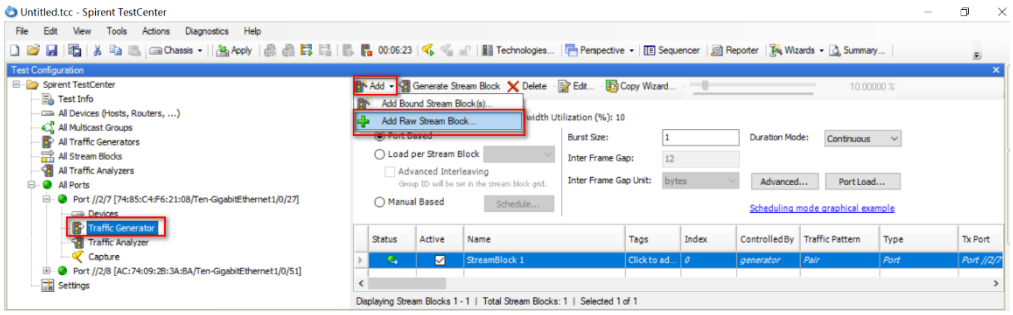
Display stp brief

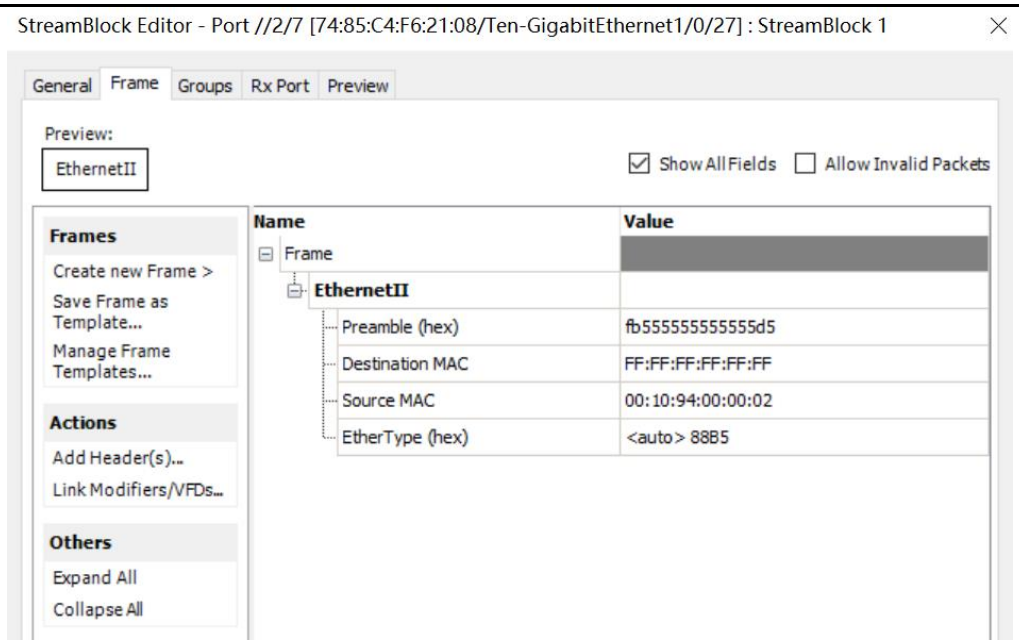
```
[DUT1]dis stp br
 MST ID   Port                                    Role  STP State     Protection
 0        Ten-GigabitEthernet1/0/25               DESI  FORWARDING    NONE
 0        Ten-GigabitEthernet1/0/26               ROOT  FORWARDING    NONE
 0        Ten-GigabitEthernet1/0/27               DESI  FORWARDING    NONE
```

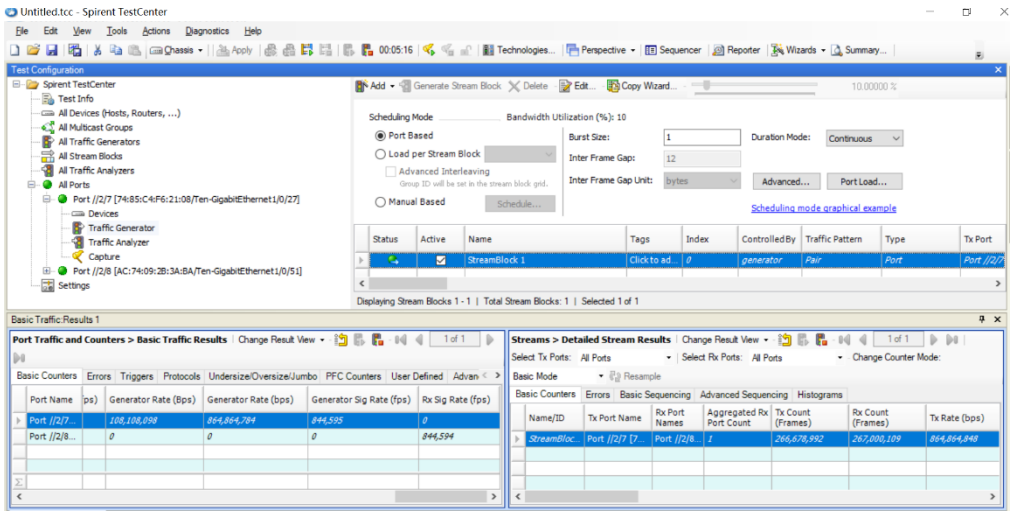
```
[DUT2]dis stp br
 MST ID   Port                                    Role  STP State     Protection
 0        Ten-GigabitEthernet1/0/49               ALTE  DISCARDING    NONE
 0        Ten-GigabitEthernet1/0/50               ROOT  FORWARDING    NONE
 0        Ten-GigabitEthernet1/0/51               DESI  FORWARDING    NONE
```

```
[DUT3]dis stp br
 MST ID   Port                                    Role  STP State     Protection
 0        Ten-GigabitEthernet1/0/24               DESI  FORWARDING    NONE
 0        Ten-GigabitEthernet1/0/39               DESI  FORWARDING    NONE
```

4. Send broadcast traffic and no broadcast storm occurs.



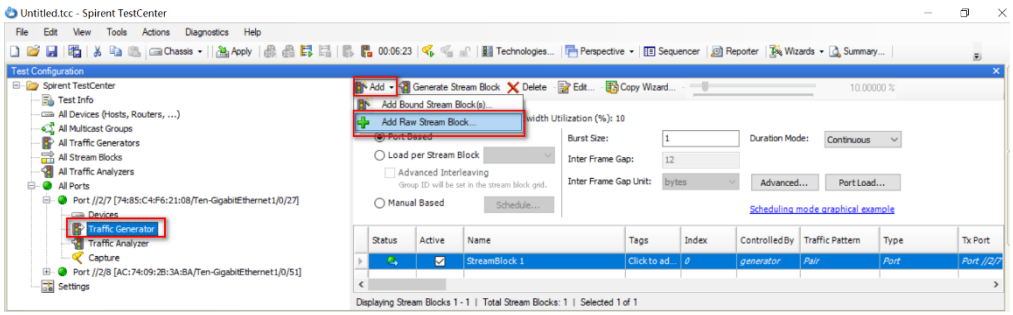


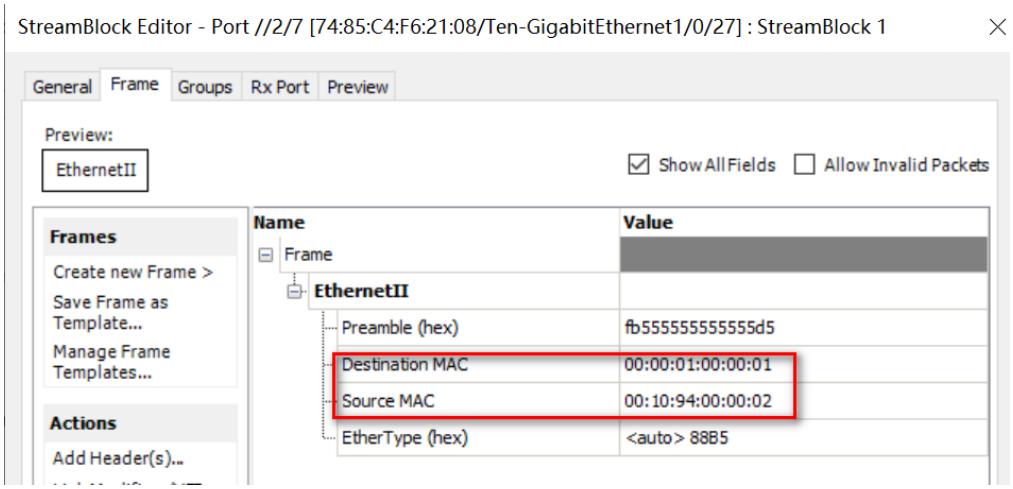


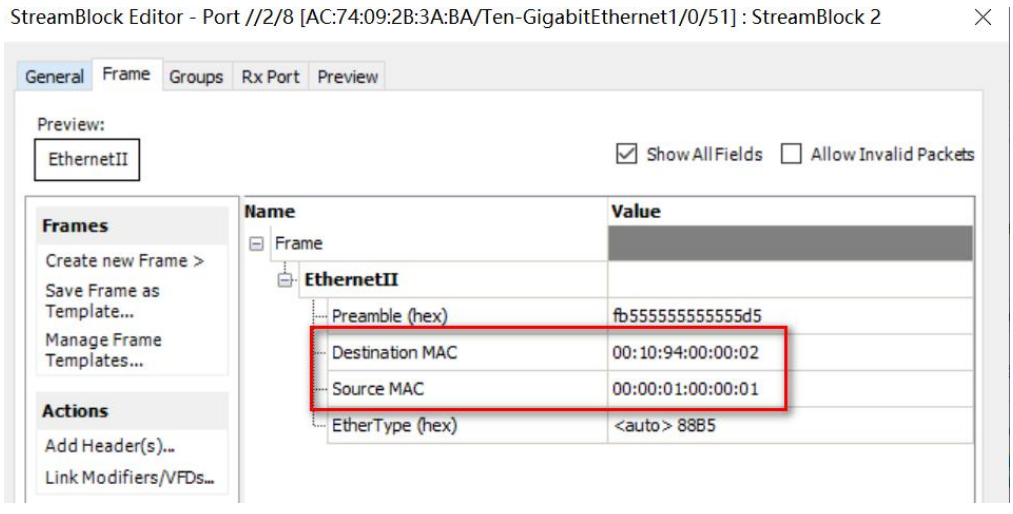
Display counter rate inbound interface

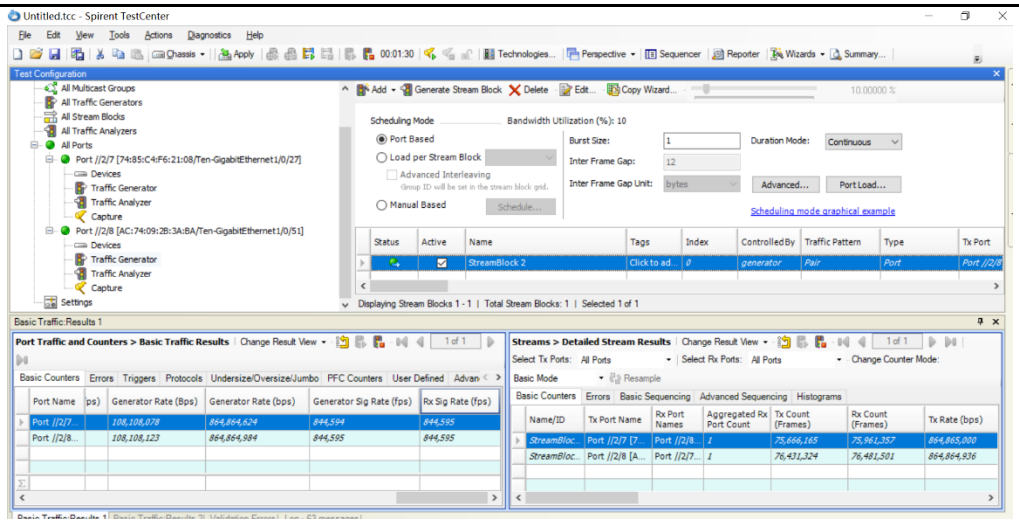
```
[DUT1]d c r  i i
Usage: Bandwidth utilization in percentage
Interface            Usage (%)    Total (pps)    Broadcast (pps)    Multicast (pps)
XGE1/0/25                   0              0                 --                 --
XGE1/0/26                   0              0                 --                 --
XGE1/0/27                  10         844575                 --                 --

 Overflow: More than 14 digits.
       --: Not supported.
[DUT1]d c r o i
Usage: Bandwidth utilization in percentage
Interface            Usage (%)    Total (pps)    Broadcast (pps)    Multicast (pps)
XGE1/0/25                  10         844575                 --                 --
XGE1/0/26                  10         844575                 --                 --
XGE1/0/27                   0              0                 --                 --

 Overflow: More than 14 digits.
       --: Not supported.
```

5. Send bi-direction unicast traffic and no traffic loss occurs.



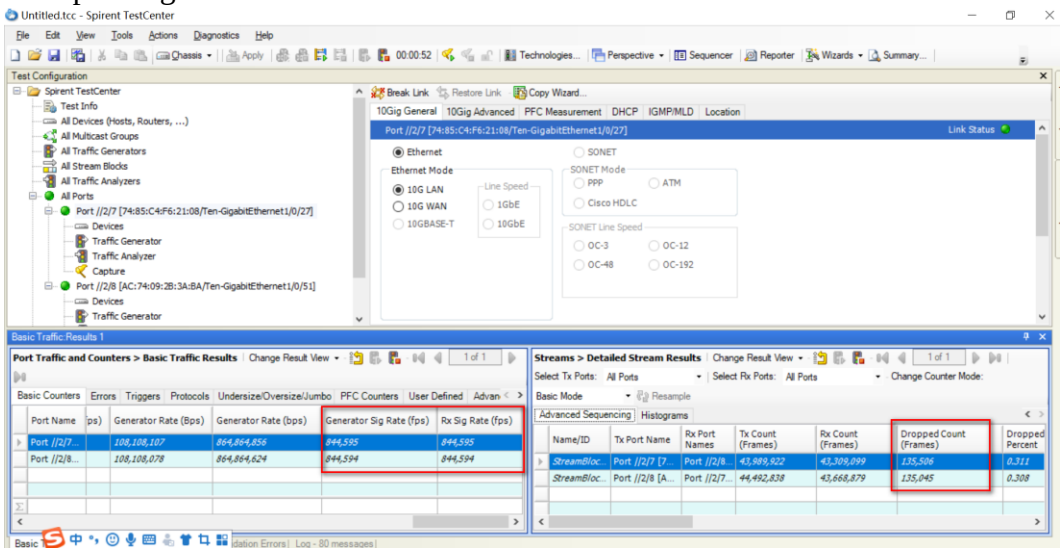






6. Remove the link between DUT1 and DUT2

7. Traffic is interrupted within 2 seconds, and the DUTs can recalculate spanning trees.

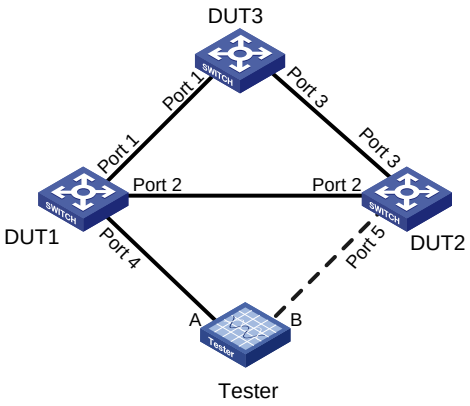


135506/844594=0.158 s

☐ Passed	☐ Failed

2.3 MSTP

Test Item Name: MSTP
Work Hour: 50 min
Test Topology:



Test Process:

1. On the DUTs, create VLAN 2, configure the ports that interconnect the DUTs as trunk ports, and configure the ports to permit packets of all VLANs.
2. On the DUTs, configure an MSTP region, and map VLAN 1 and VLAN 2 to MSTI 1 and MSTI 2, respectively.
3. Configure Port 4 of DUT 1 and Port 5 of DUT 2 as edge ports.
4. Configure DUT 1 as the root bridge of MSTI 0 and MSTI 1, and configure DUT 3 as the root bridge of MSTI 2.
5. On the tester, send broadcast traffic of VLAN 1 continuously through Port A, and send broadcast traffic of VLAN 2 continuously through Port B. Result 1 is expected.
6. Remove the link between DUT 1 and DUT 2. Result 2 is expected.
7. Reconnect DUT 1 to DUT 2. Result 2 is expected.
8. Remove the link between DUT 1 and DUT 3. Result 3 is expected.
9. Reconnect DUT 1 to DUT 3. Result 3 is expected.

Expect Results:

1. Port A and Port B of the tester send and receive traffic correctly.
2. On Port B, incoming traffic is interrupted for fewer than 2 seconds. No traffic interruption occurs on Port A.
3. On Port A, incoming traffic is interrupted for fewer than 2 seconds. No traffic interruption occurs on Port B.

Actual Result:

1. On the DUTs, create VLAN 2, configure the ports that interconnect the DUTs as trunk ports, and configure the ports to permit packets of all VLANs.

#

vlan 2

#

interface Ten-GigabitEthernet1/0/xx

port link-mode bridge

port link-type trunk

port trunk permit vlan all

#

2. On the DUTs, configure an MSTP region, and map VLAN 1 and VLAN 2 to MSTI 1 and MSTI 2, respectively.

[DUT] stp region-configuration

[DUT-mst-region] instance 1 vlan 1

[DUT-mst-region] instance 2 vlan 2

[DUT-mst-region] region-name H3C

[DUT-mst-region] active region-configuration

3. Configure Port 4 of DUT 1 and Port 5 of DUT 2 as edge ports.

#

interface Ten-GigabitEthernet1/0/27

port link-mode bridge

port link-type trunk

port trunk permit vlan all

stp edged-port

#

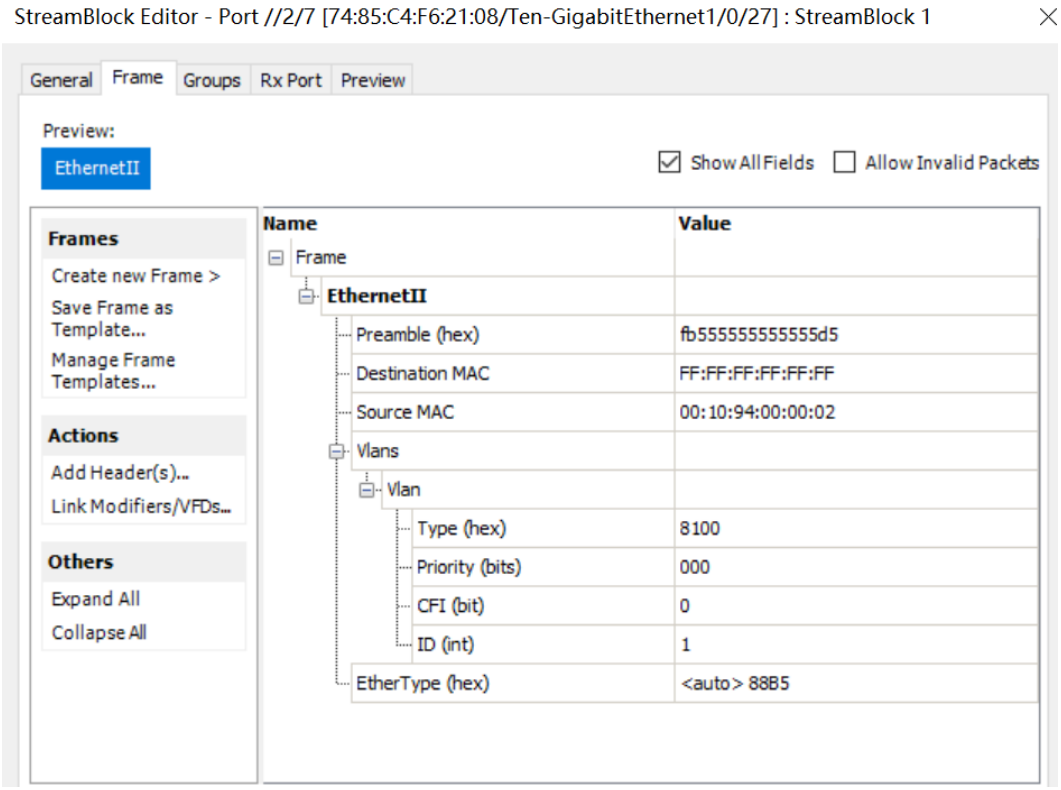
4. Configure DUT 1 as the root bridge of MSTI 0 and MSTI 1, and configure DUT 3 as the root bridge of MSTI 2.

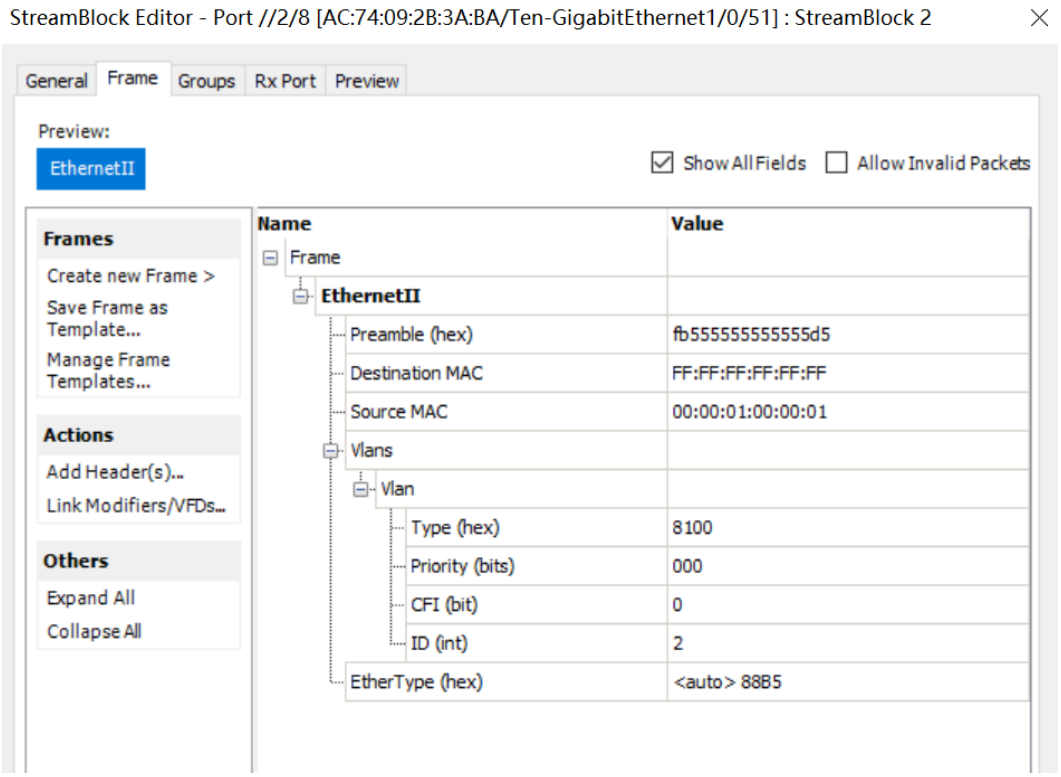
[DUT1]stp instance 0 root primary

[DUT1]stp instance 1 root primary

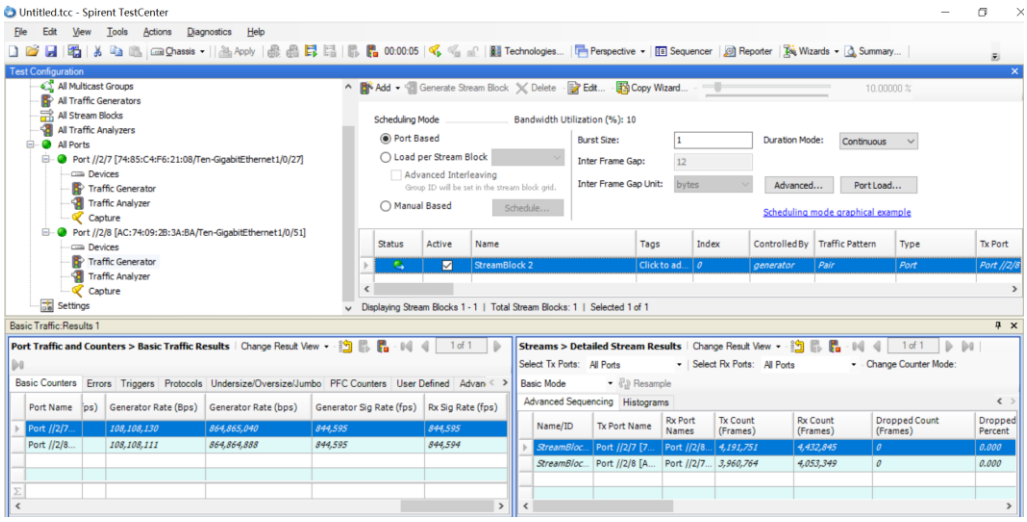
[DUT3]stp instance 2 root primary

5. Send broadcast traffic of VLAN 1 continuously through Port A, and send broadcast traffic of VLAN 2 continuously through Port B

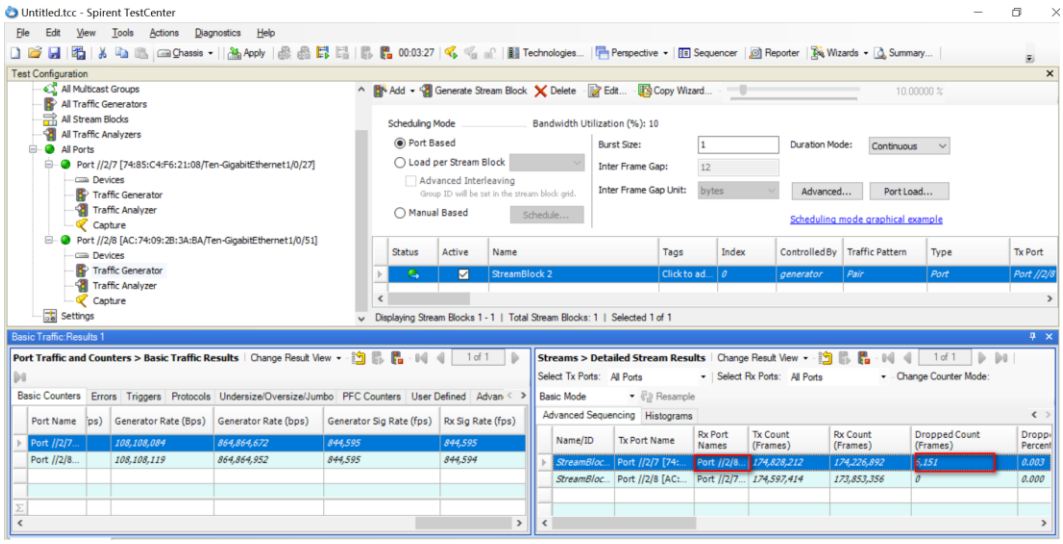




6. Port A and Port B of the tester send and receive traffic correctly.

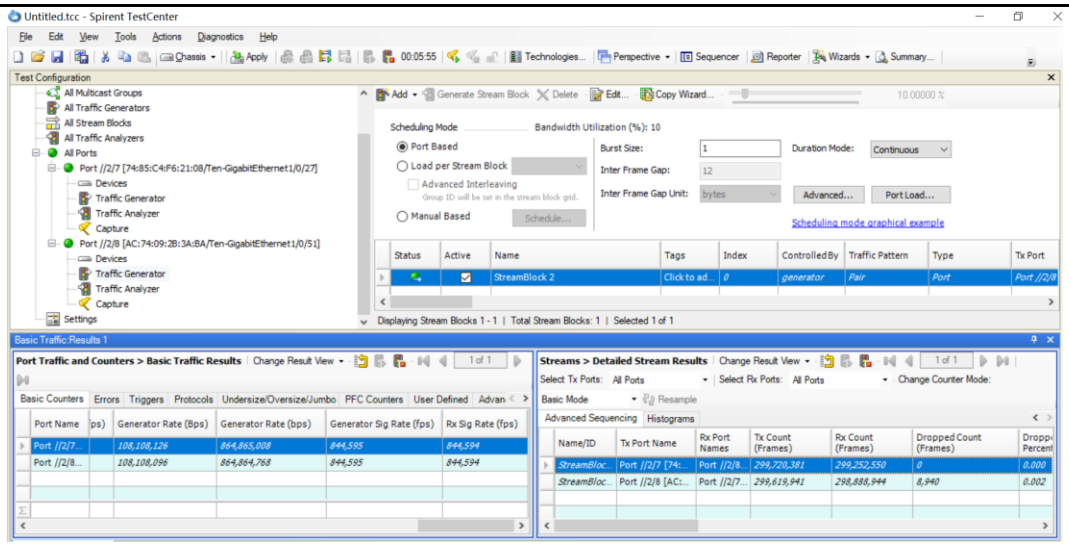


7. Remove and reconnect the link between DUT1 and DUT2
8. On Port B, incoming traffic is interrupted within 2 seconds. No traffic interruption occurs on Port A.



6151/844594=0.00728 s

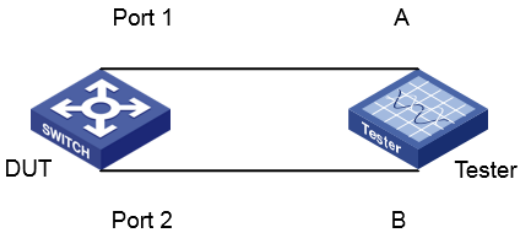
9. Remove and reconnect the link between DUT1 and DUT3
10. On Port A, incoming traffic is interrupted within 2 seconds. No traffic interruption occurs on Port B.



8940/844595=0.01058 s

☐ Passed	☐ Failed

2.4 VLAN specification

Test Item Name: VLAN Specification
Work Hour: 30 min
Test Topology: 
Test Process: 1. Create 4094 VLANs on DUT 2. Configure Port 1 and Port 2 as trunk Ports and configure them to permit all VLANs 3. The Tester Port A sends 4094 L2 broadcast packets in burst mode. The VLAN tag of the sent message range from 1 to 4094. The packet is received and captured on Port B. The expected result is 1.
Expect Results:

1. Tester Port B can receive 4,094 L2 broadcast messages from Port A

Actual Result：

1. Create 4094 VLANs on DUT

```
[DUT]vlan all
Please wait..........Done.
[DUT]
```

2. Configure ports as trunk mode and permit all VLANs to pass

#

interface GigabitEthernet1/0/1

port link-mode bridge

port link-type trunk

port trunk permit vlan all

#

interface GigabitEthernet1/0/2

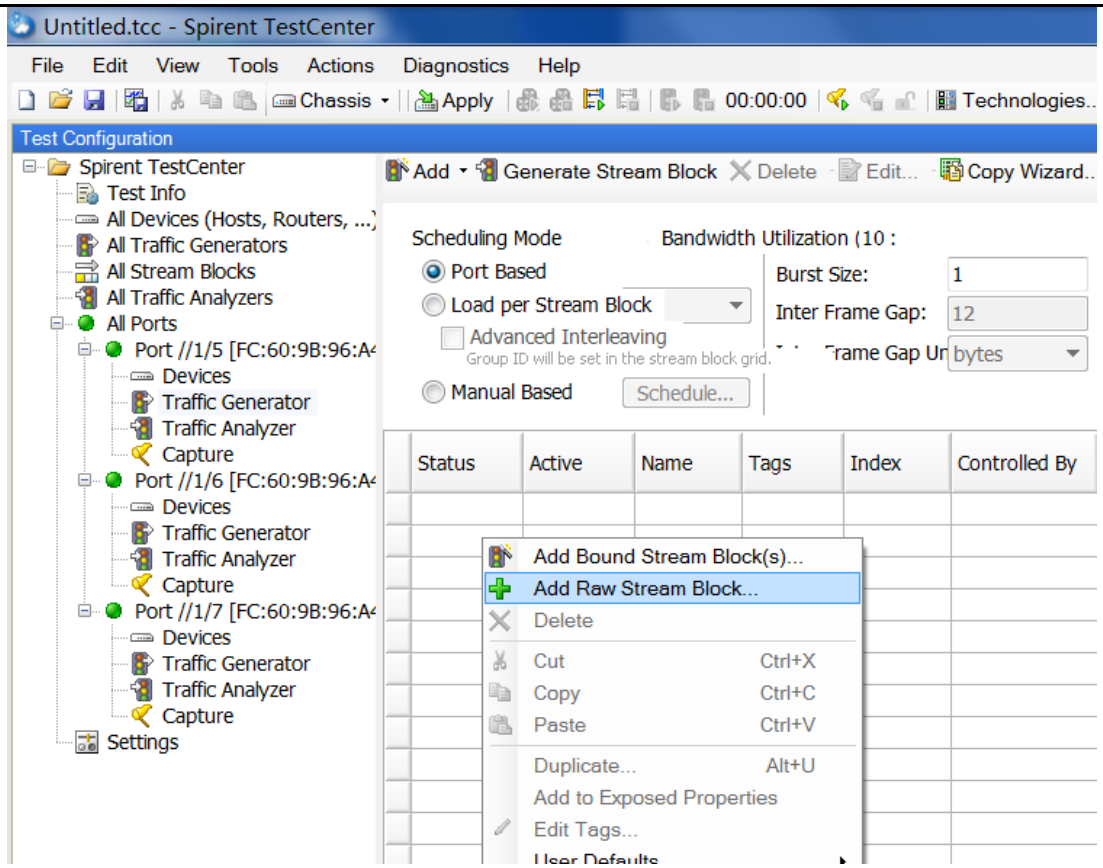
port link-mode bridge

port link-type trunk

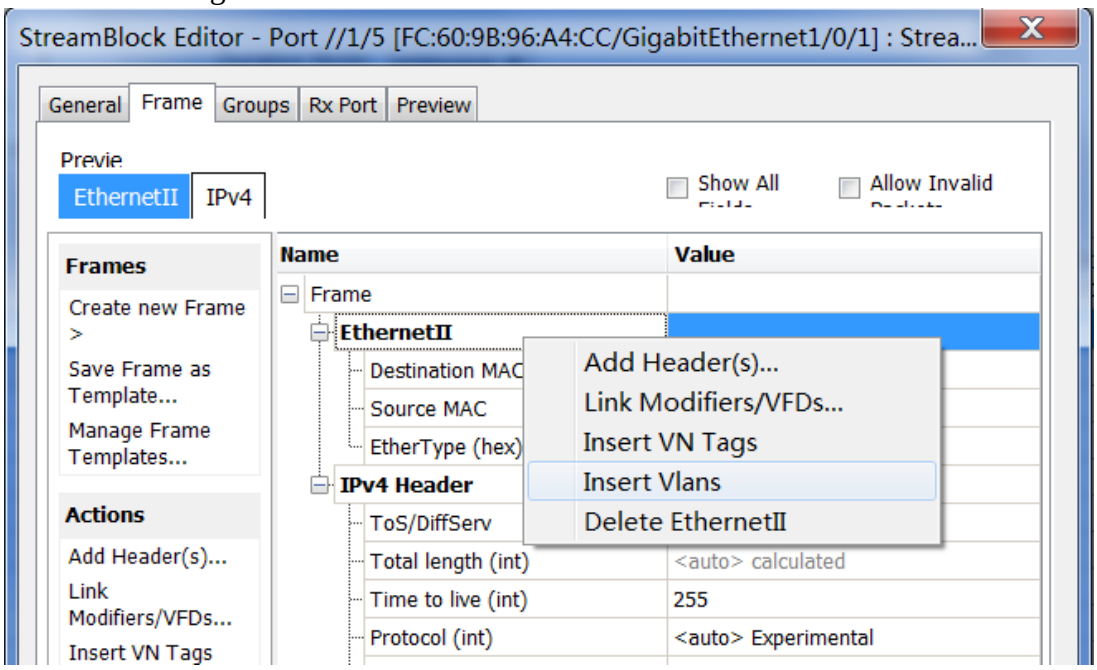
port trunk permit vlan all

#

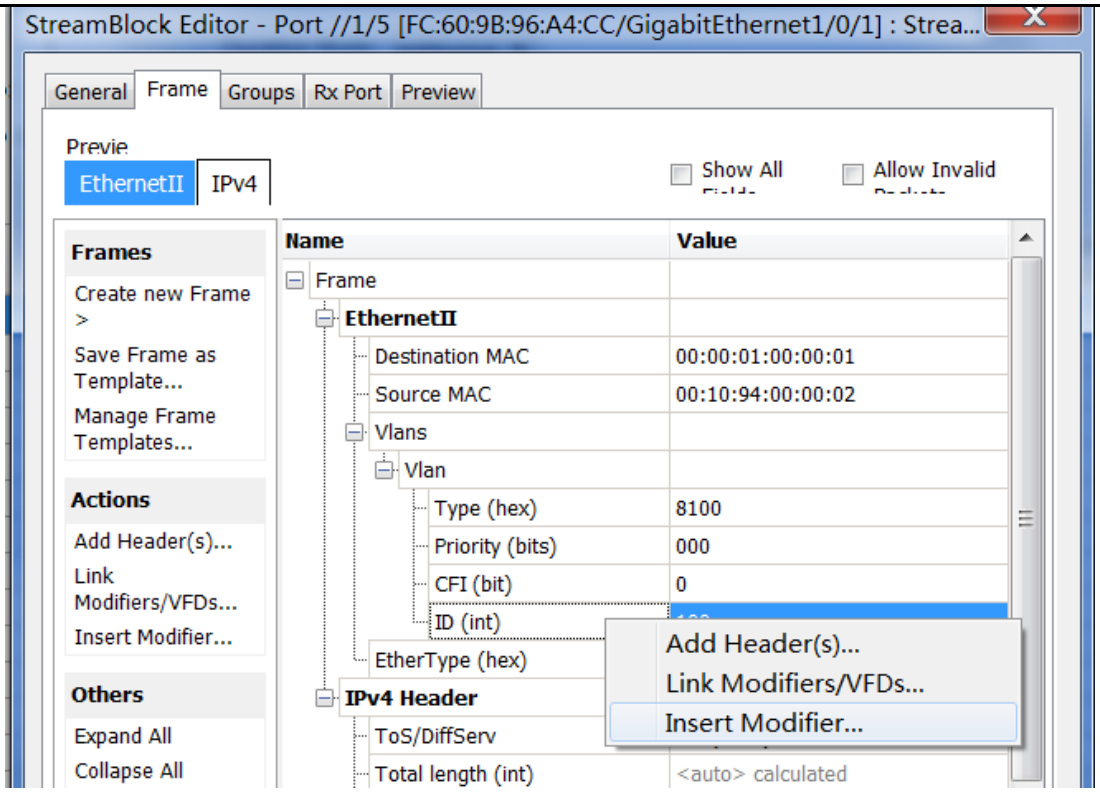
4. Create raw stream on TC1:

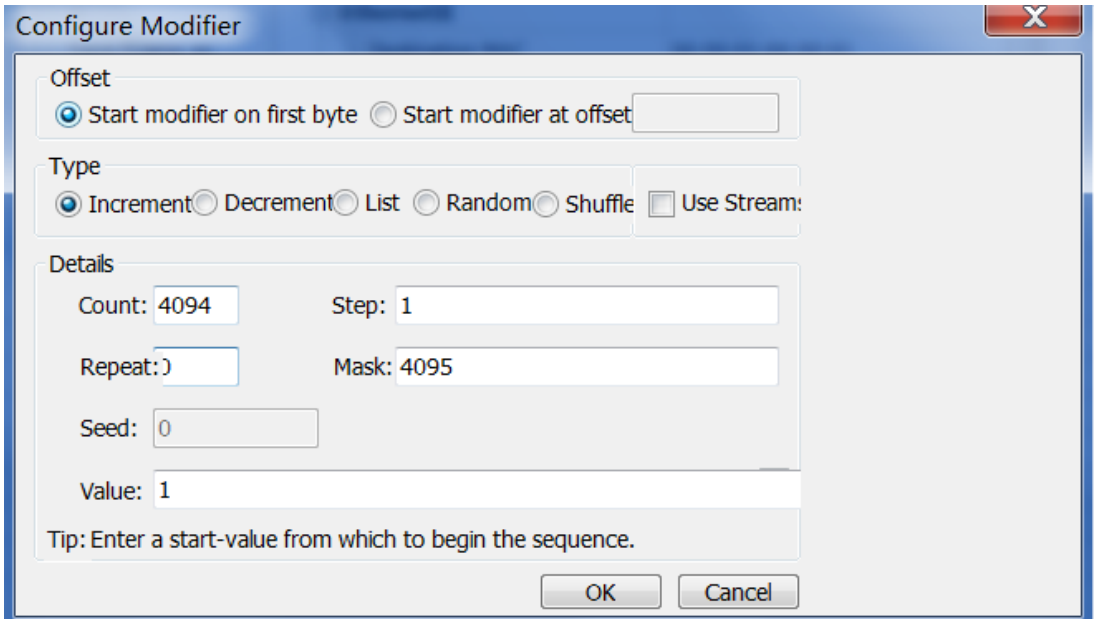


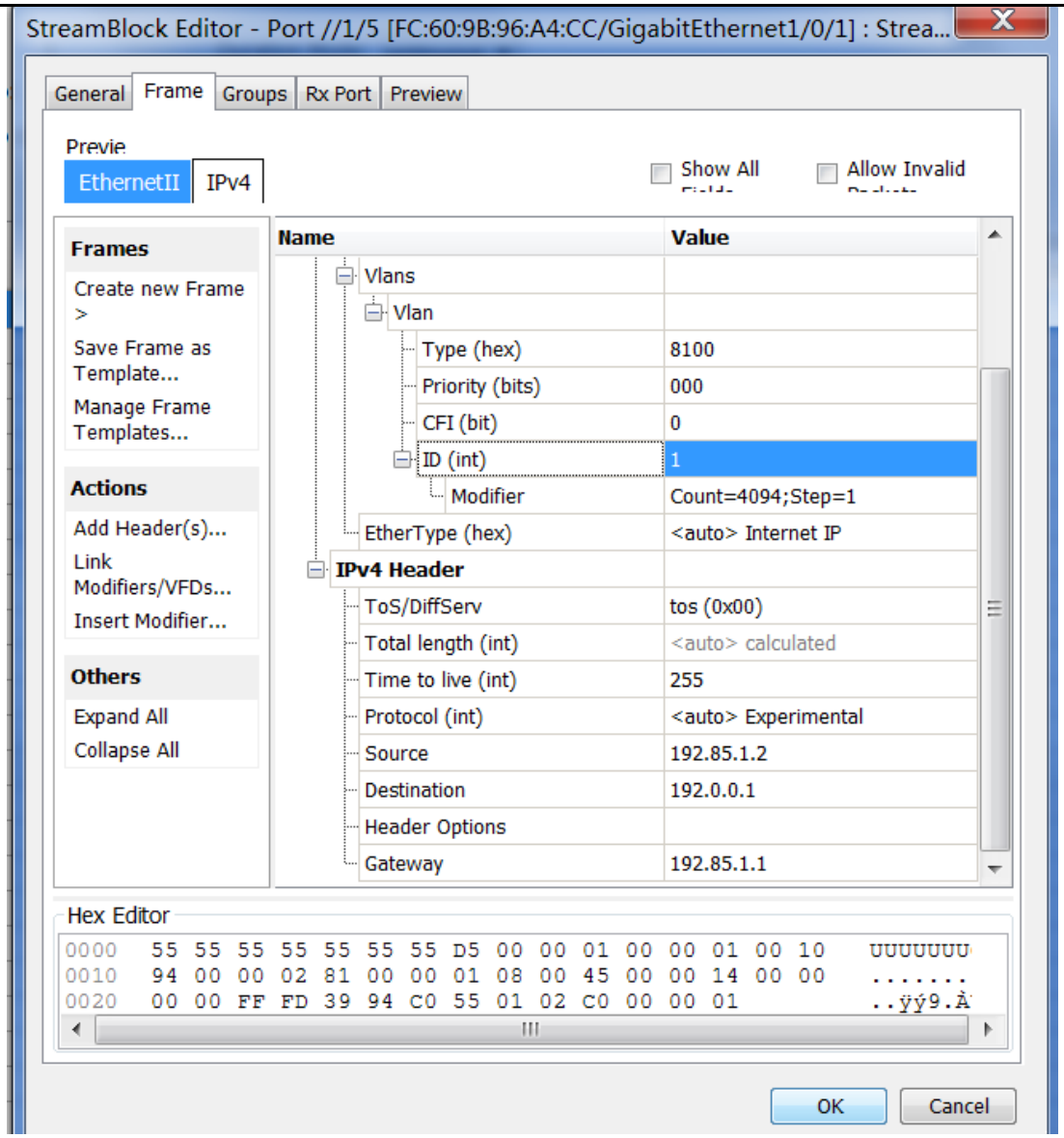
5. Add vlan tags to the traffic



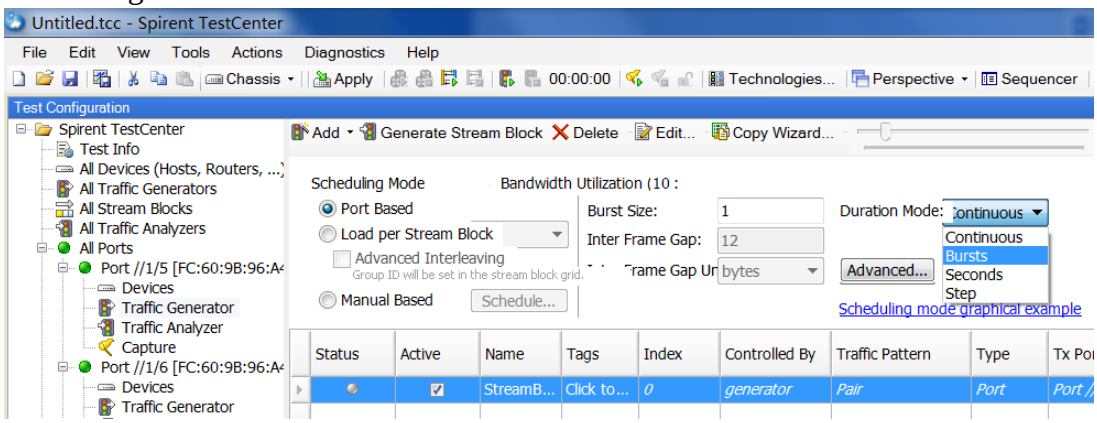
6. Change the vlan modifier:



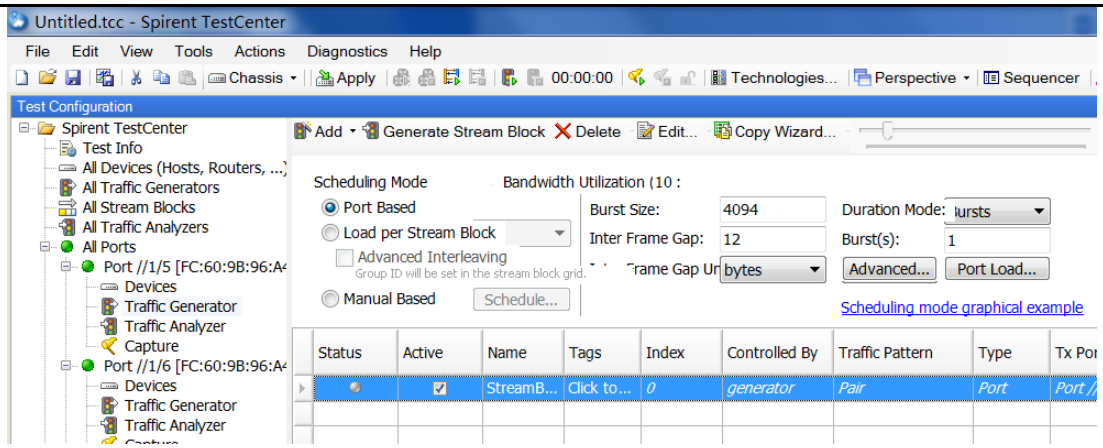




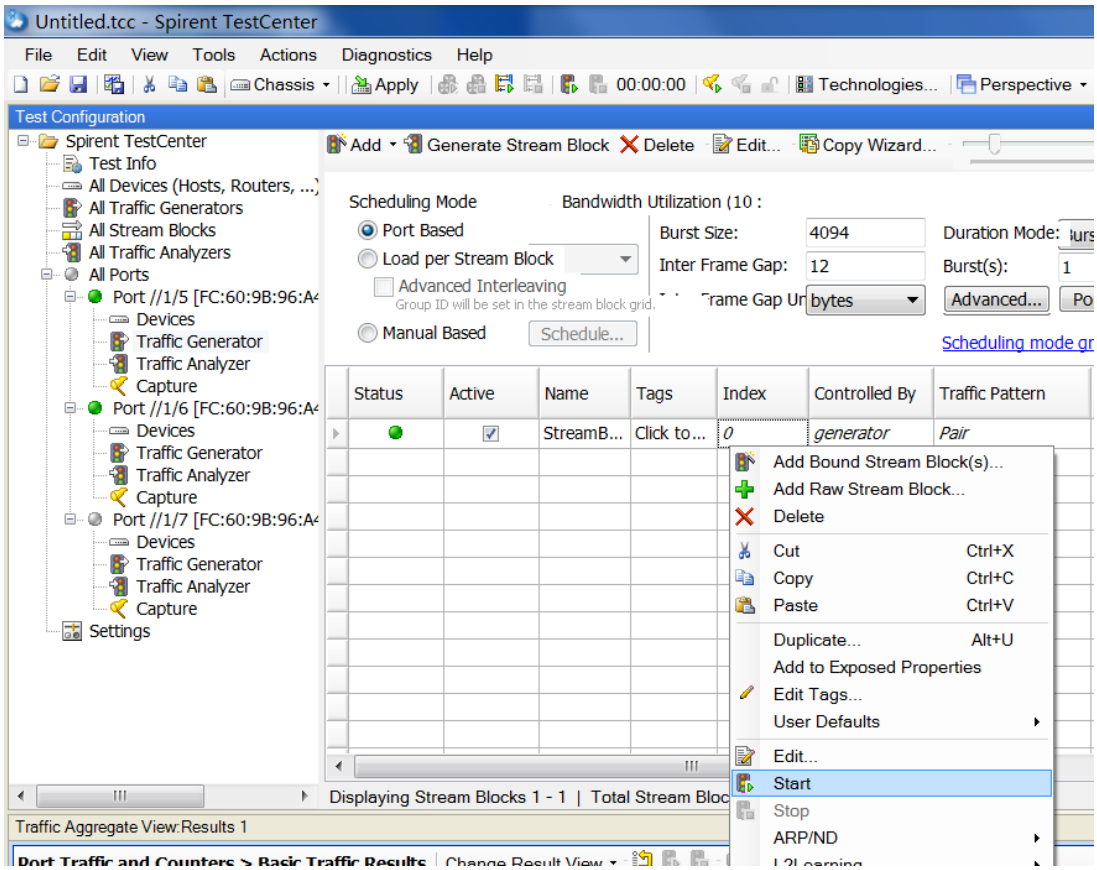
7. Change the duration mode to burst:



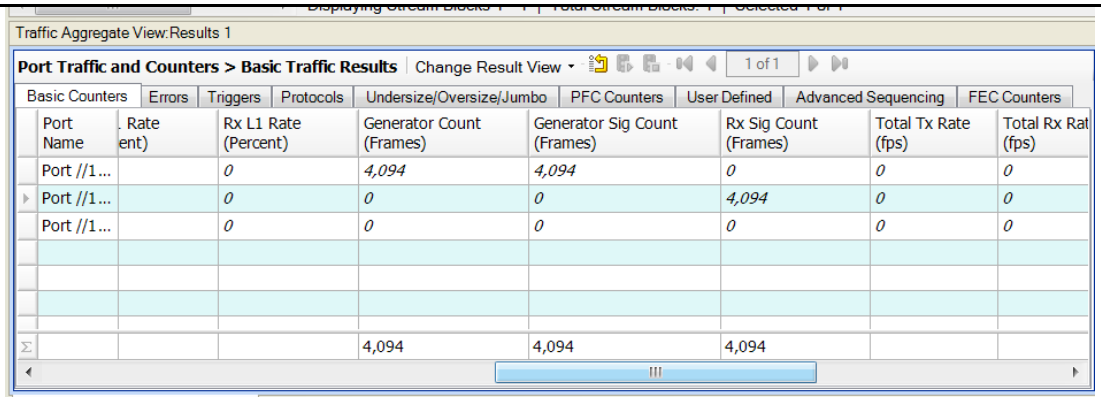
8. Change the burst size to 4094



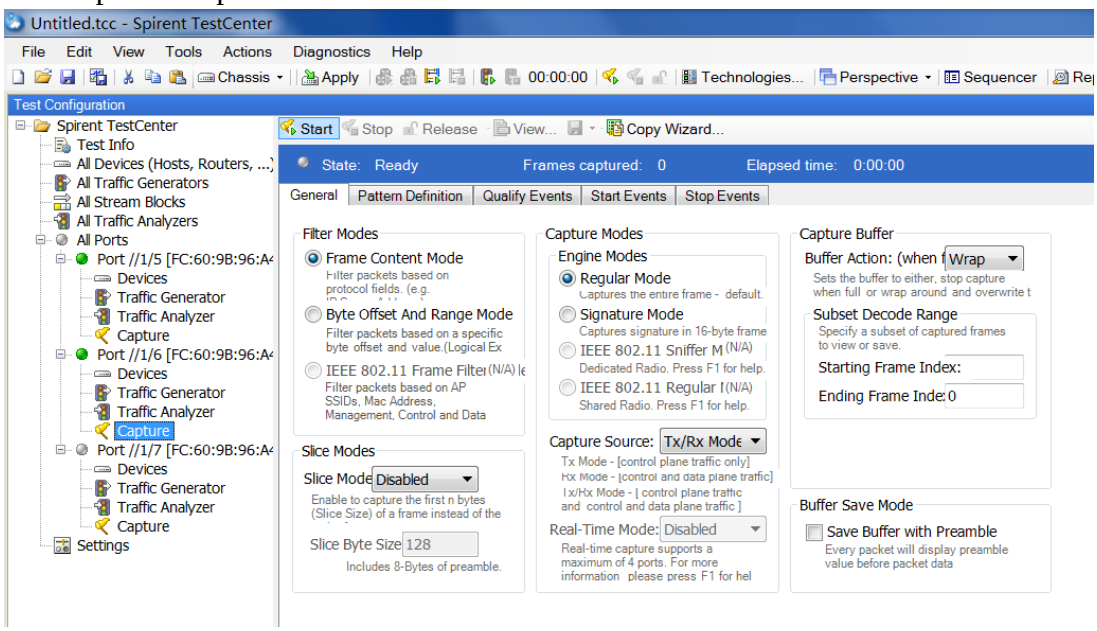
9. Start the traffic



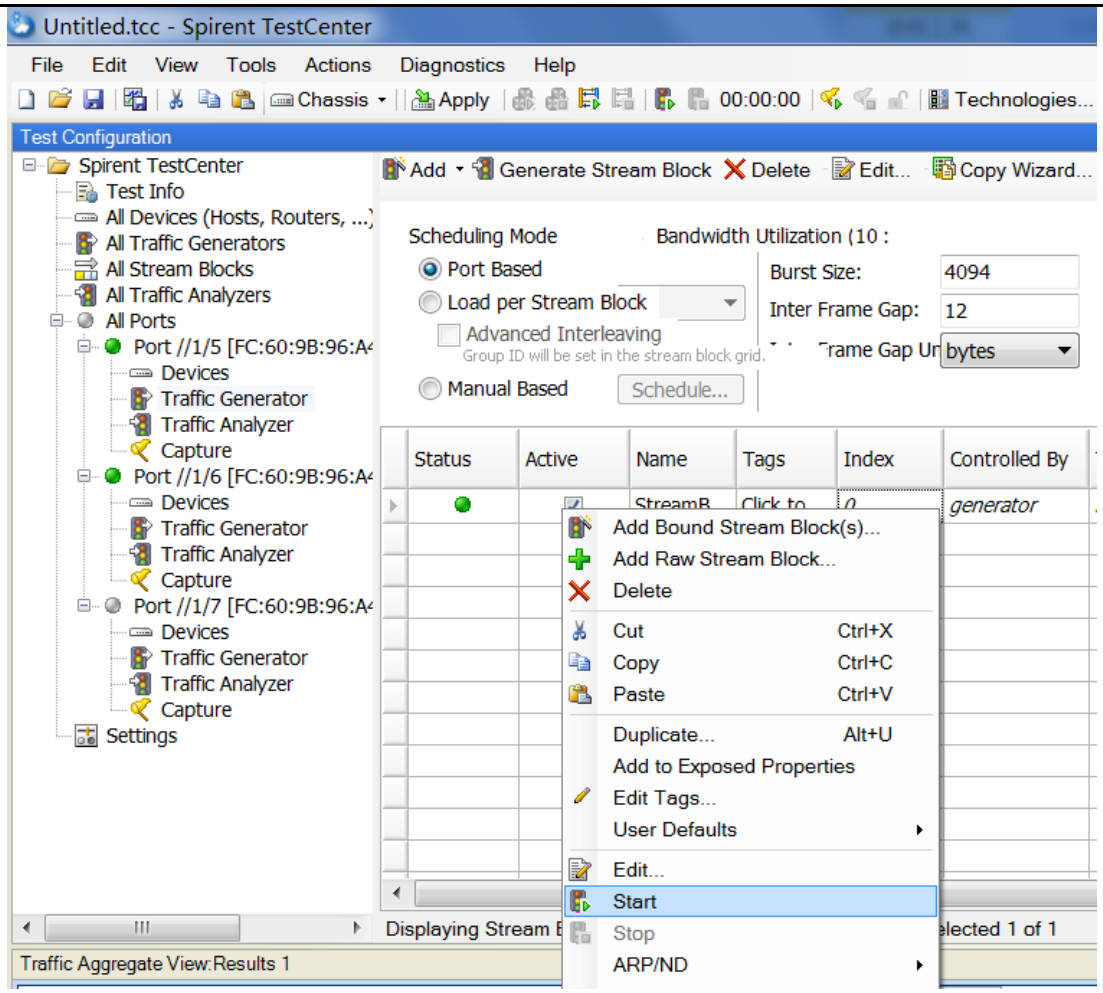
10. Check the result, there are 4094 packets sent and received



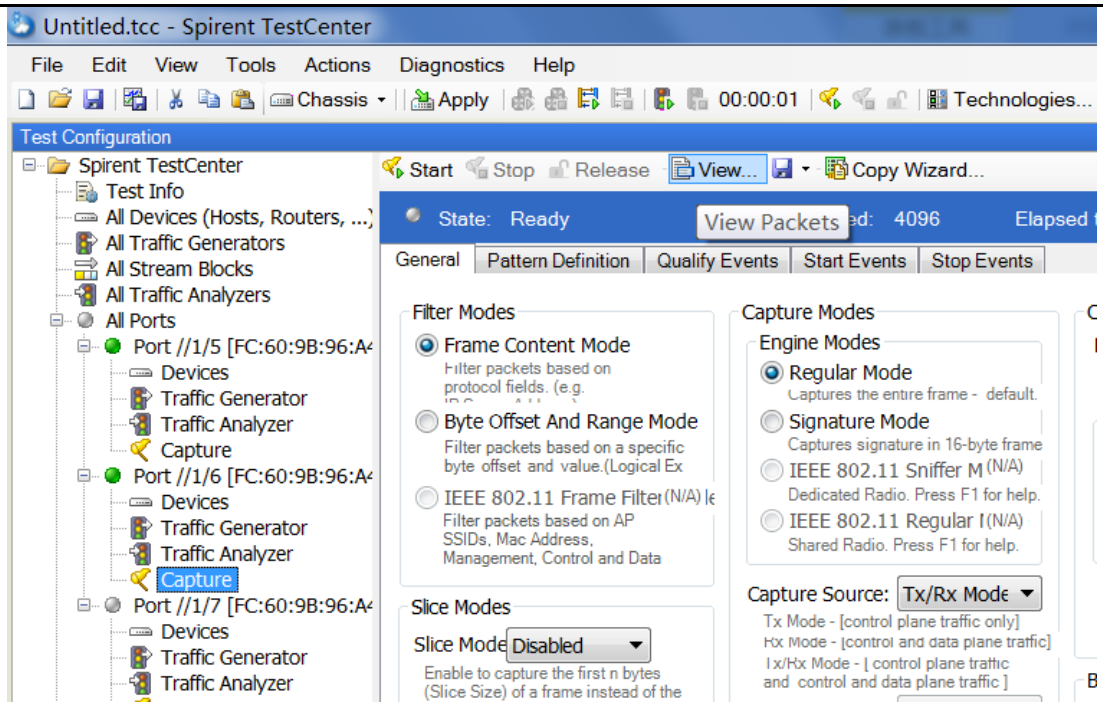
11. Capture the packets on TC2



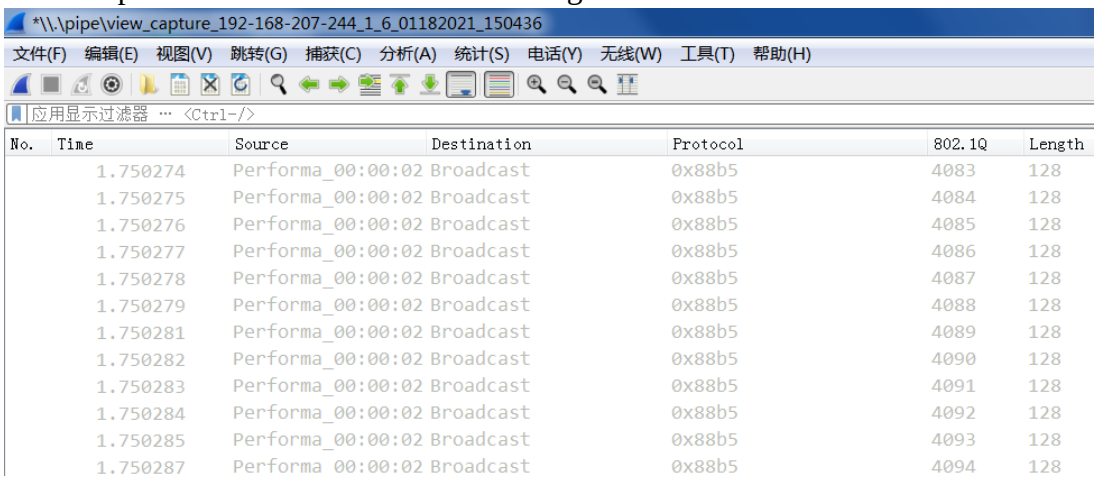
12. Send the traffic again and stop the capture



13. Check the results



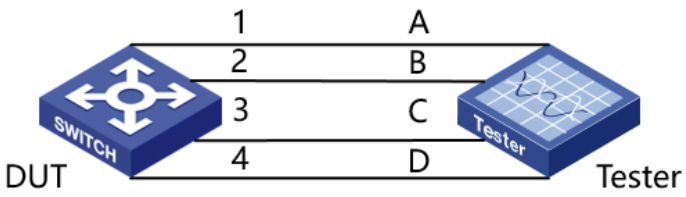
14. The packets have 4094 different vlan tags



☐ Passed	☐ Failed

2.5 Isolate group

Test Item Name: Isolate group
Work Hour：20 min
Test Purpose:
Test Topology:



Test Process:

1. Assign Port1 through Port 4 to VLAN 2. Create isolation group 1, and assign Port 1 through Port3 to isolation group 1. Do not assign Port4 to the isolation group.
2. Send broadcast packets out of Port A of Tester. Result 1 is expected.
3. Send broadcast packets out of Port B of Tester. Result 1 is expected.
4. Send broadcast packets out of Port C of Tester. Result 1 is expected.
5. Send broadcast packets out of Port D of Tester. Result 2 is expected.

Expect Results:

1. Only Port D of Tester receives packets.
2. Ports A, B, and C of Tester receive packets.

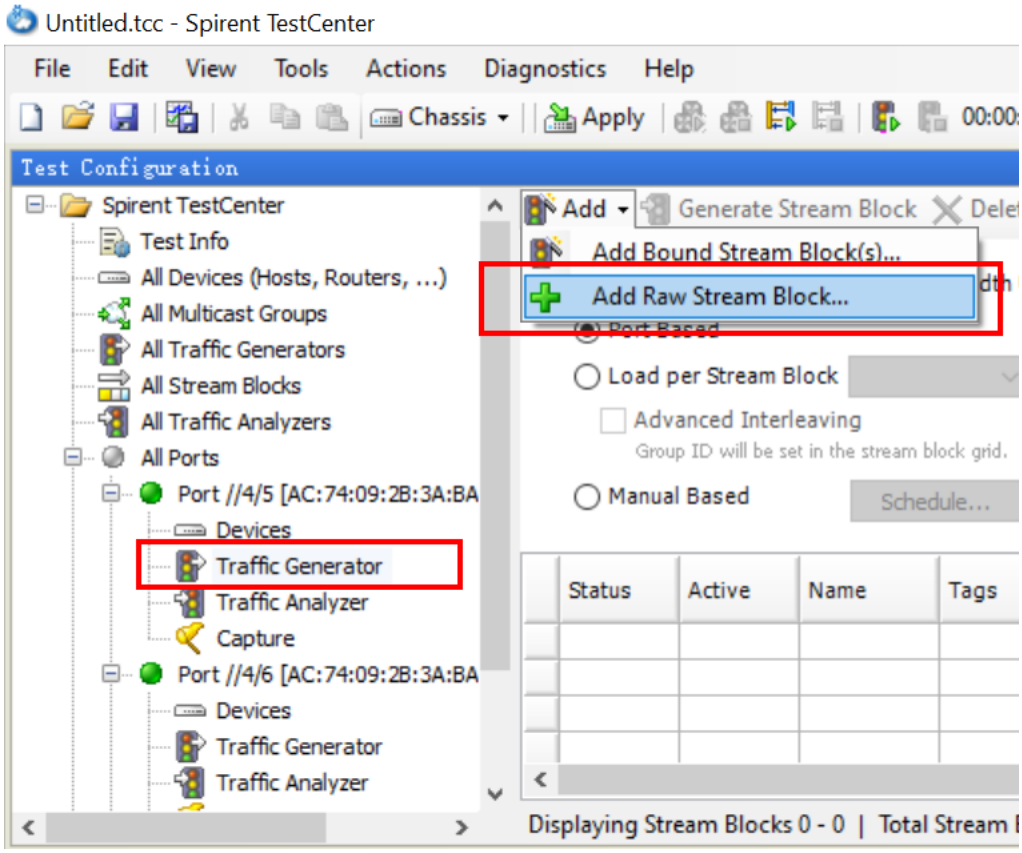
Actual Result:

1. Assign Port1 through Port 4 to VLAN 2. Create isolation group 1, and assign Port 1 through Port3 to isolation group 1. Do not assign Port4 to the isolation group.

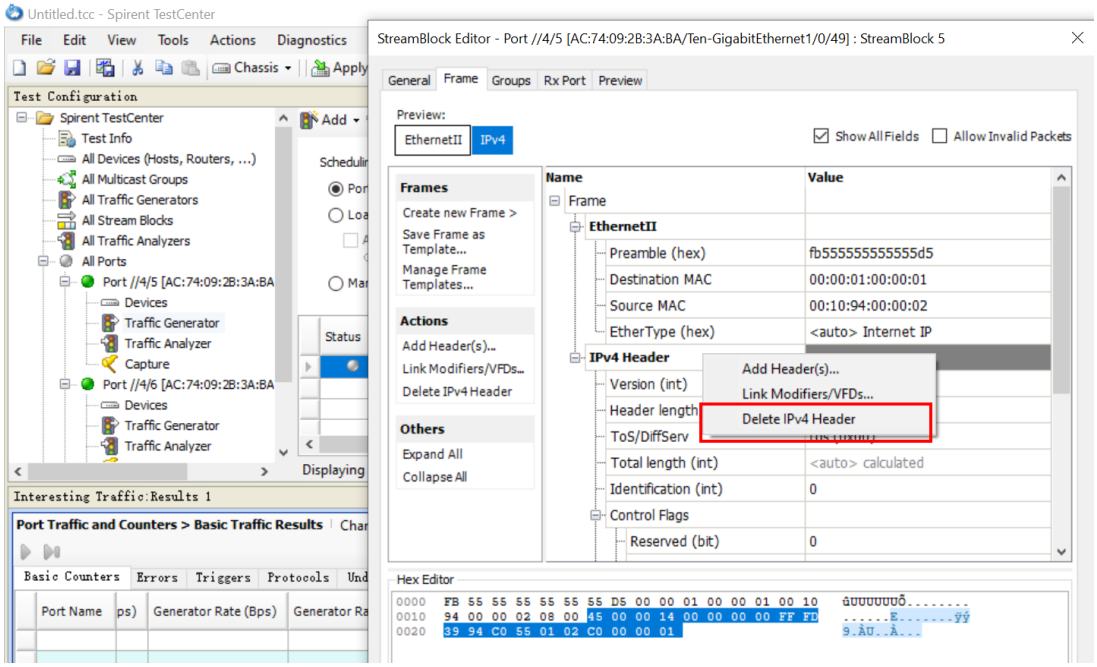
```
[DUT]port-isolate group 1
[DUT]vlan 2
[DUT-vlan2]port Ten-GigabitEthernet 1/0/49 to Ten-GigabitEthernet 1/0/52
[DUT-vlan2]quit
[DUT]interface Ten-GigabitEthernet1/0/49
[DUT-Ten-GigabitEthernet1/0/49]port-isolate enable group 1
[DUT-Ten-GigabitEthernet1/0/49]interface Ten-GigabitEthernet1/0/50
[DUT-Ten-GigabitEthernet1/0/50]port-isolate enable group 1
[DUT-Ten-GigabitEthernet1/0/50]interface Ten-GigabitEthernet1/0/51
[DUT-Ten-GigabitEthernet1/0/51]port-isolate enable group 1
```

2. Send broadcast packets out of Port A of Tester. Result 1 is expected.

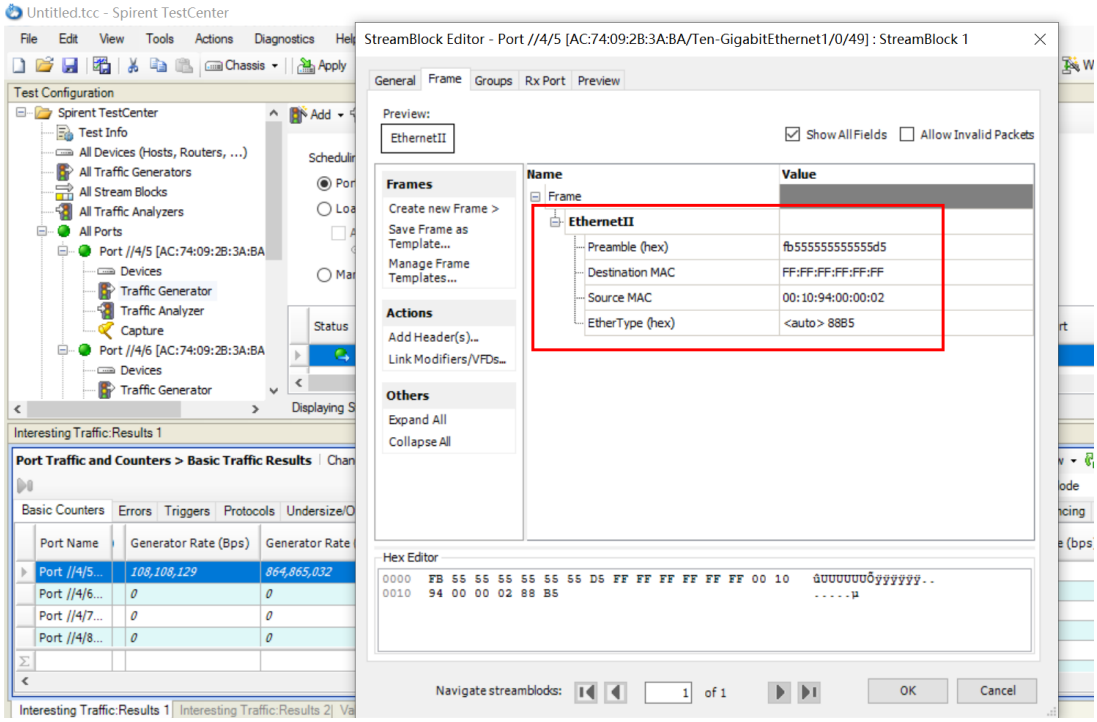
Add raw stream.



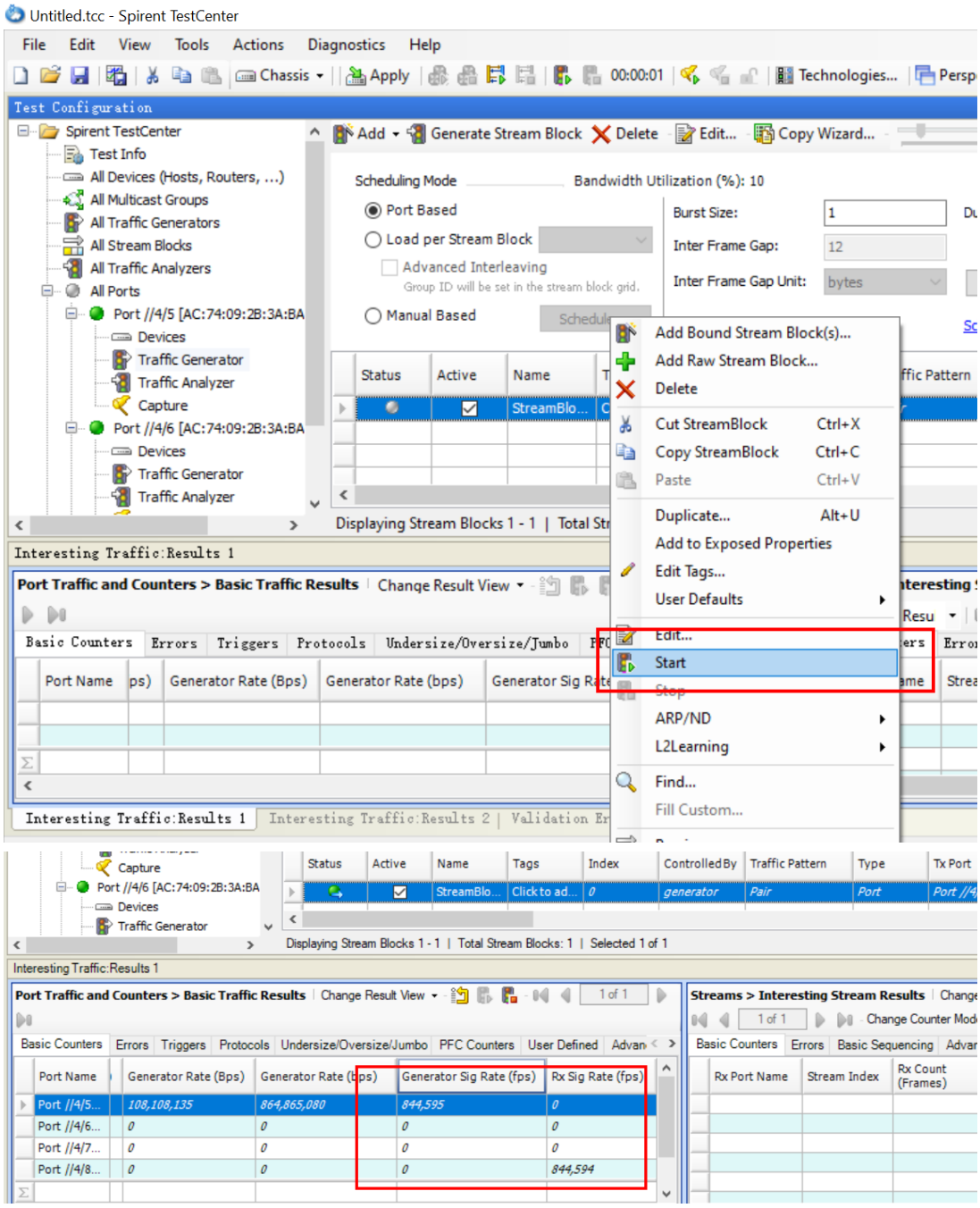
Delete the IPv4 header.



Change the destination MAC to send the broadcast traffic.

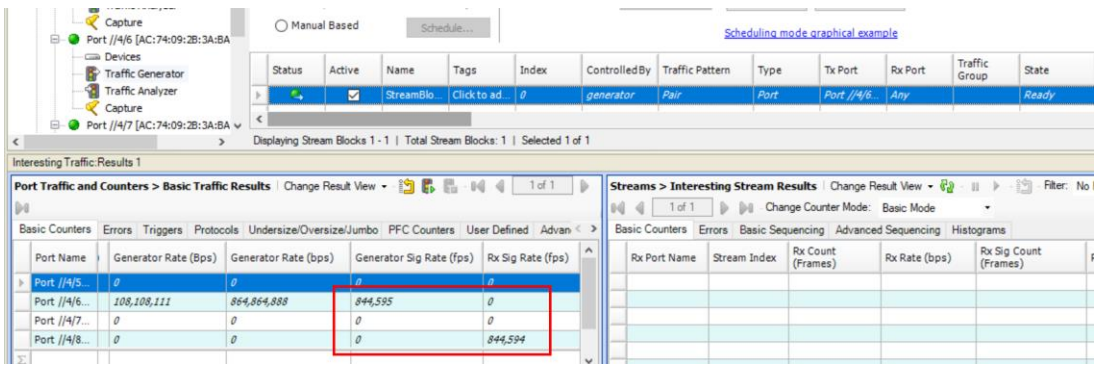


Strat to send the traffic.

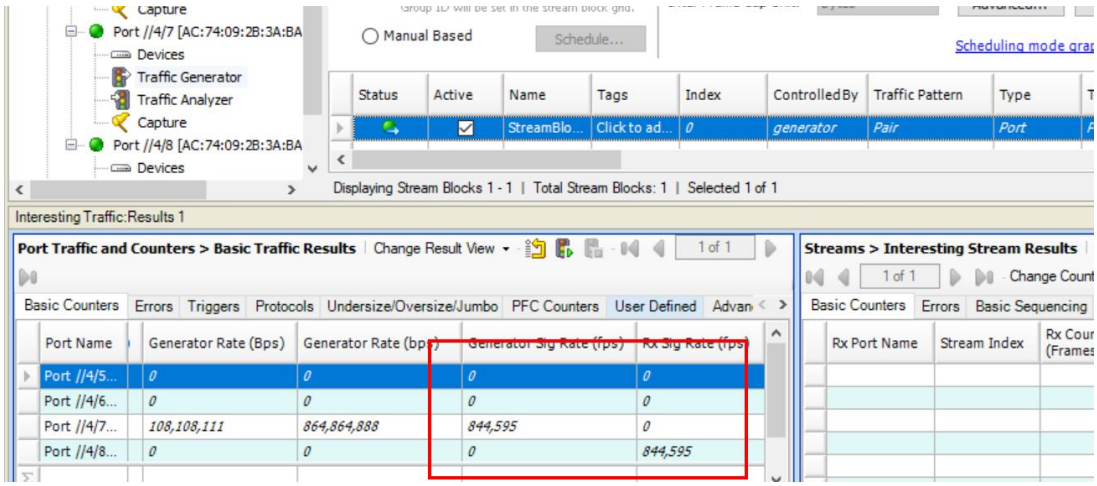


3. Send broadcast packets out of Port B of Tester. Result 1 is expected.

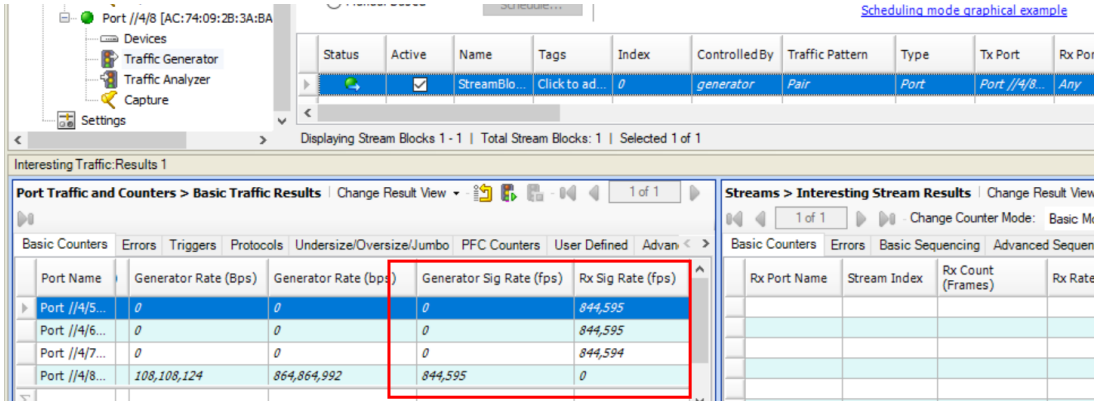
The process of creating a data stream is similar to Port A



4. Send broadcast packets out of Port C of Tester. Result 1 is expected.
The process of creating a data stream is similar to Port A.



5. Send broadcast packets out of Port D of Tester. Result 2 is expected.
The process of creating a data stream is similar to Port A.



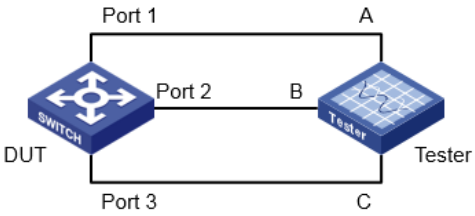
☐ Passed	☐ Failed

2.6 SPAN

Test Item Name: SPAN

Work Hour: 30 min

Test Topology:



Test Process:

1. Configure the following static MAC address entries (0-0-1111) on DUT1.
2. Send packets with destination MAC address 0-0-1111 out of Port B of Tester. Result 1 is expected.
3. Configure Port 3 to monitor bidirectional packets of Port 1 on DUT1.
4. Send packets with destination MAC address 0-0-1111 out of Port B of Tester. Result 2 is expected.

Expect Results:

1. Packets sent out Port B of Tester can't be received on Port C of Tester.
2. Packets sent out Port B of Tester can be received on Port C of Tester.

Actual Result：

1. Configure static mac-address on Port 1 and configure Port 1/2 to vlan 100

#

interface GigabitEthernet1/0/1

port link-mode bridge

port access vlan 100

mac-address static 0000-0000-1111 vlan 100

#

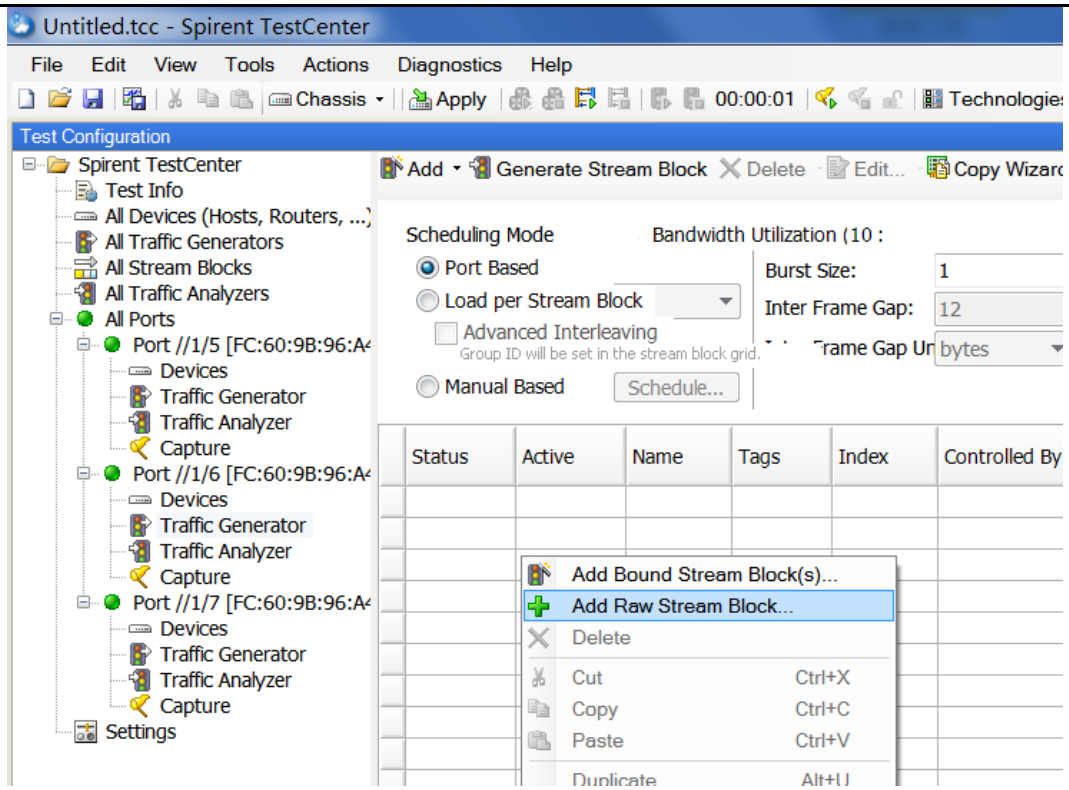
interface GigabitEthernet1/0/2

port link-mode bridge

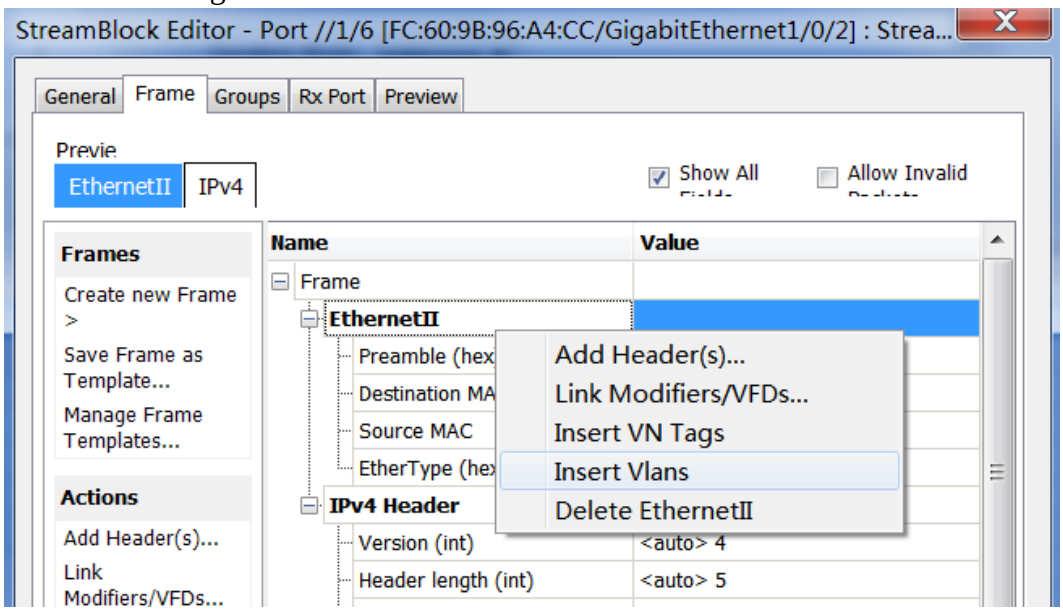
port access vlan 100

#

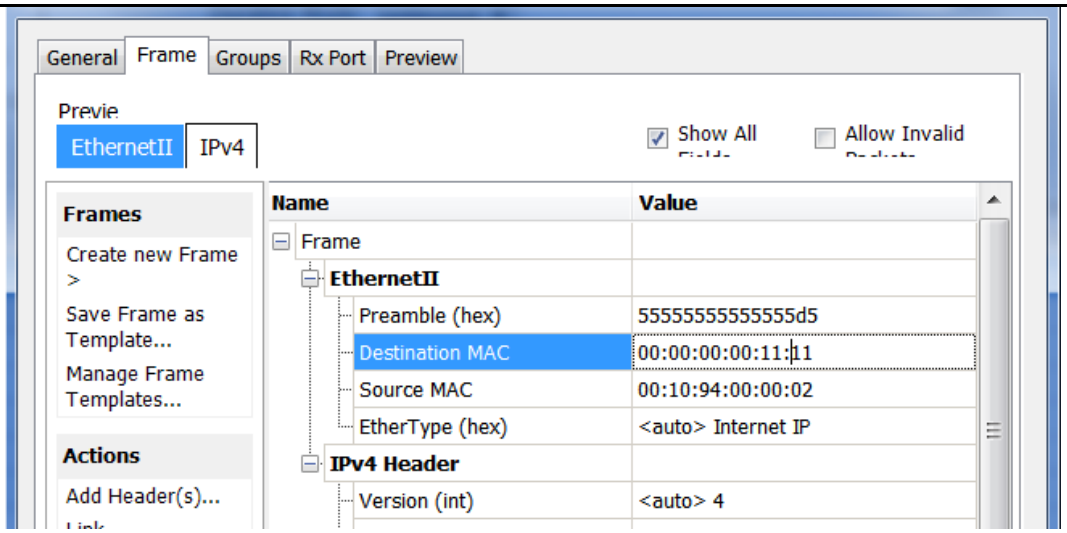
2. Create raw stream



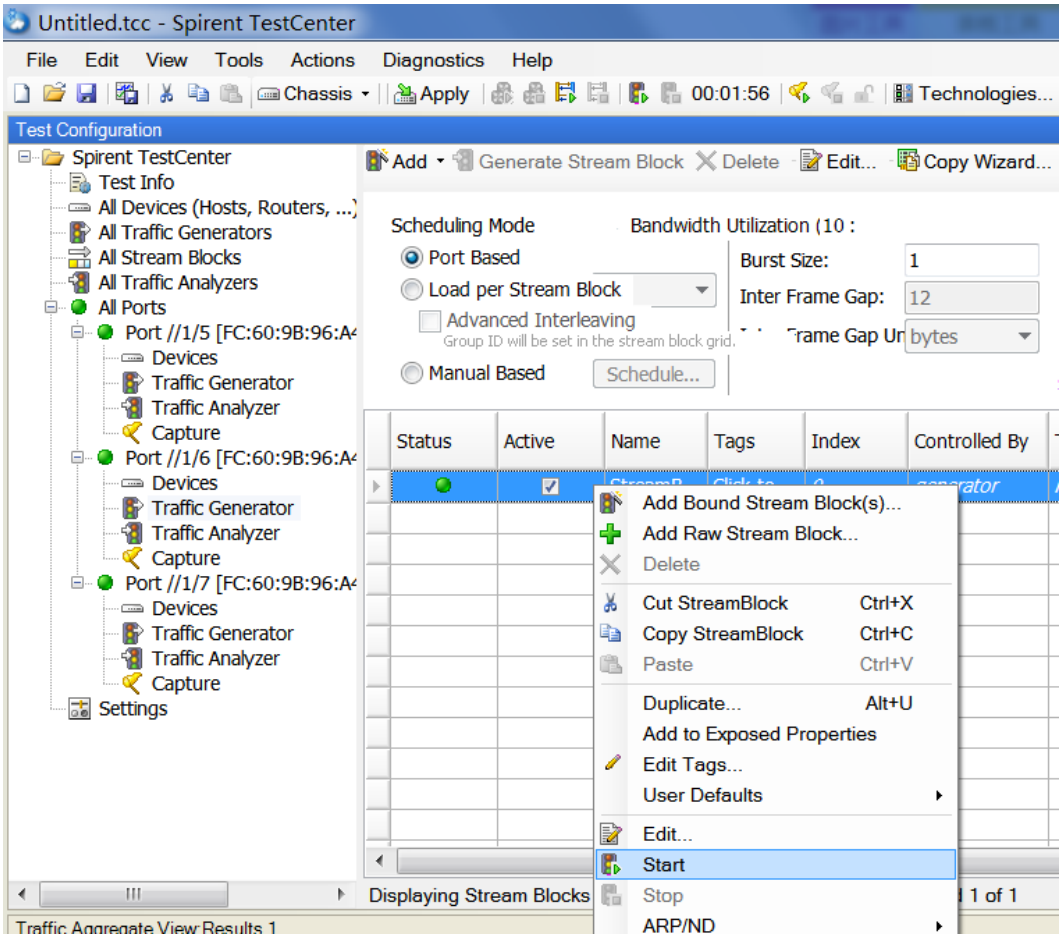
3. Add vlan tag for the stream

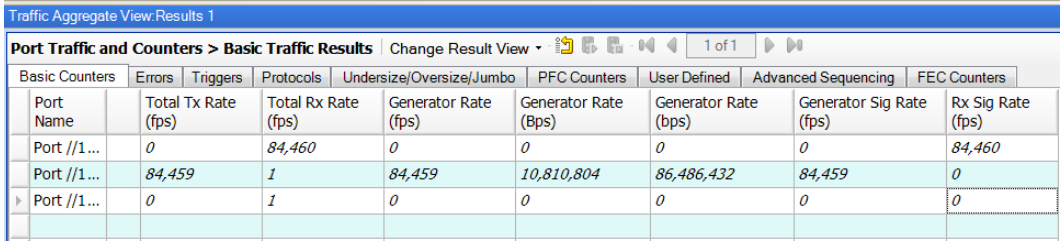


4. Change the destination mac and click on **OK**



5. Start the traffic and check the result





Port Name	Total Tx Rate (fps)	Total Rx Rate (fps)	Generator Rate (fps)	Generator Rate (Bps)	Generator Rate (bps)	Generator Sig Rate (fps)	Rx Sig Rate (fps)
Port //1...	0	84,460	0	0	0	0	84,460
Port //1...	84,459	1	84,459	10,810,804	86,486,432	84,459	0
Port //1...	0	1	0	0	0	0	0

All the traffic is received on Port A and isn't received on Port C

6. Configure Port 3 to monitor bidirectional packets of Port 1 on DUT1.

#

interface GigabitEthernet1/0/1

port link-mode bridge

port access vlan 100

mac-address static 0000-0000-1111 vlan 100

mirroring-group 1 mirroring-port both

#

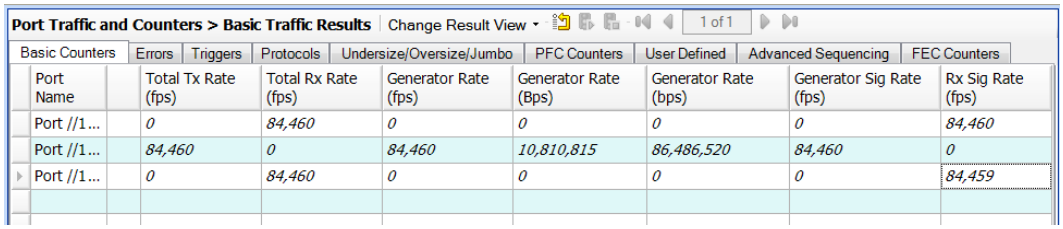
interface GigabitEthernet1/0/3

port link-mode bridge

mirroring-group 1 monitor-port

#

7. Start the traffic and check the result



Port Name	Total Tx Rate (fps)	Total Rx Rate (fps)	Generator Rate (fps)	Generator Rate (Bps)	Generator Rate (bps)	Generator Sig Rate (fps)	Rx Sig Rate (fps)
Port //1...	0	84,460	0	0	0	0	84,460
Port //1...	84,460	0	84,460	10,810,815	86,486,520	84,460	0
Port //1...	0	84,460	0	0	0	0	84,459

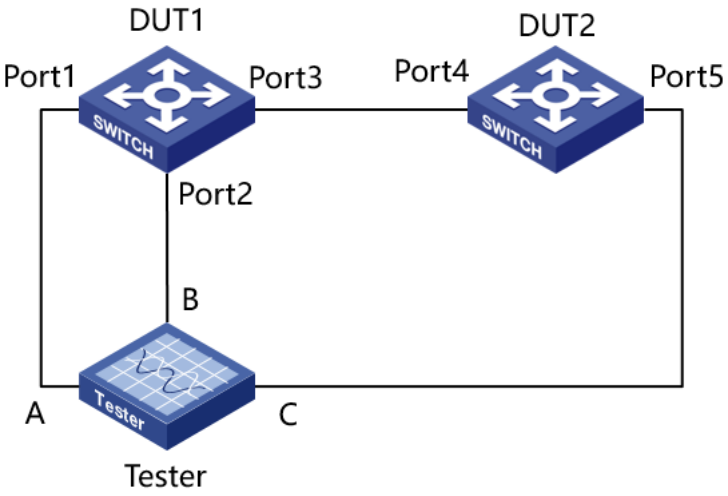
The traffic is received on Port A and Port C

☐ Passed	☐ Failed

2.7 RSPAN

Test Item Name: RSPAN
Work Hour：30 min

Test Topology:



Test Process:

1. Configure a remote source group to mirror the inbound packets of the specified source Port and configure a remote probe VLAN for the remote source group on DUT1.
2. Configure DUT2.
3. Configure the following static MAC address entries (0-0-1111/0-0-2222) on DUT1.
4. Send packets with destination MAC address 0-0-2222 out of Port A of Tester.
5. Send packets with destination MAC address 0-0-1111 out of Port B of Tester.
6. Result 1 is expected.
7. Configure mirroring group 1 to monitor bidirectional packets of Port 1. Send packets with destination MAC address 0-0-2222 out of Port A of Tester. Send packets with destination MAC address 0-0-1111 out of Port B of Tester. Result 2 is expected.
8. Configure mirroring group 1 to monitor outbound packets of Port 1. Send packets with destination MAC address 0-0-2222 out of Port A of Tester. Send packets with destination MAC address 0-0-1111 out of Port B of Tester. Result 3 is expected.

Expect Results:

1. Packets sent out Port A of Tester are received on Port C of Tester.
2. Packets sent out Port A and Port B of Tester are received on Port C of Tester.

3. Packets sent out Port B of Tester are received on Port C of Tester.

Actual Result:

1. Configure a remote source group to mirror the inbound packets of the specified source Port and configure a remote probe VLAN for the remote source group on DUT1.

```
[DUT1]vlan 100
```

```
[DUT1]mirroring-group 1 remote-source
[DUT1]mirroring-group 1 remote-probe vlan 100
[DUT1]mirroring-group 1 mirroring-port Ten-GigabitEthernet 1/0/49 inbound
[DUT1]mirroring-group 1 monitor-egress Ten-GigabitEthernet 1/0/52
```

```
[DUT1]interface Ten-GigabitEthernet1/0/52
[DUT1-Ten-GigabitEthernet1/0/52]port link-type trunk
[DUT1-Ten-GigabitEthernet1/0/52]port trunk permit vlan 100
```

2. Configure DUT2.

```
[DUT2]vlan 100
```

```
[DUT2]interface Ten-GigabitEthernet1/0/25
[DUT2-Ten-GigabitEthernet1/0/25]port link-type trunk
[DUT2-Ten-GigabitEthernet1/0/25]port trunk permit vlan 100
```

```
[DUT2]interface Ten-GigabitEthernet1/0/28
[DUT2-Ten-GigabitEthernet1/0/28]port link-type trunk
[DUT2-Ten-GigabitEthernet1/0/28]port trunk permit vlan 100
```

```
[DUT2]mirroring-group 1 remote-destination
[DUT2]mirroring-group 1 remote-probe vlan 100
Make sure the VLAN has not been used for any other purpose. Mirrored packets wi
ll be broadcast within the VLAN after the configuration. Continue? [Y/N]: y
[DUT2]mirroring-group 1 monitor-port Ten-GigabitEthernet 1/0/25
```

3. Configure the following static MAC address entries (0-0-1111/0-0-2222) on DUT1.

Send packets with destination MAC address 0-0-2222 out of Port A of Tester.

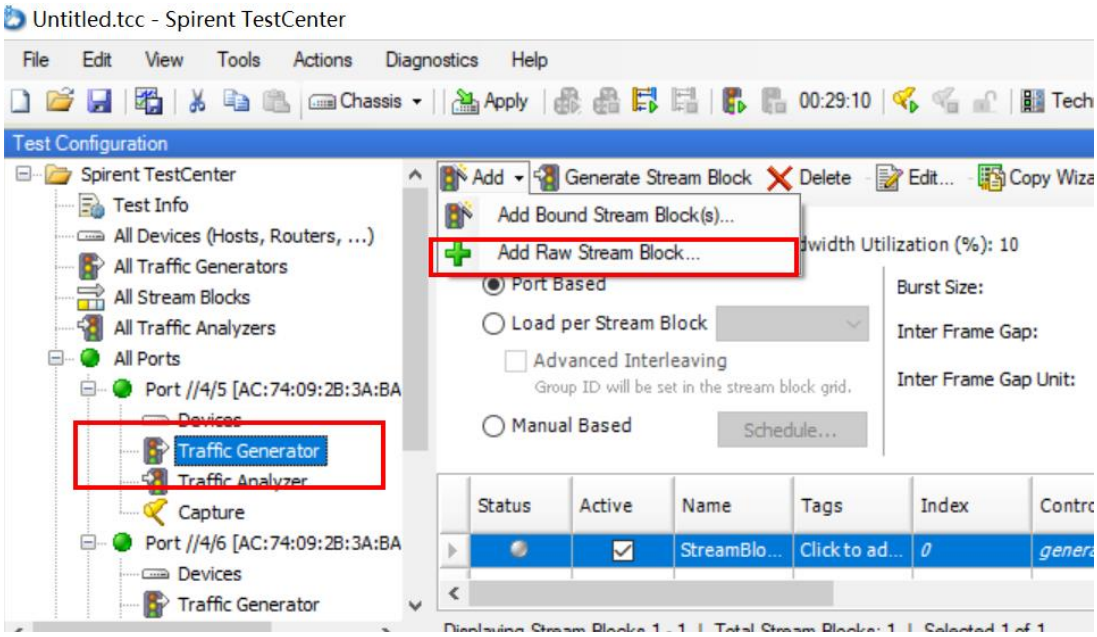
Send packets with destination MAC address 0-0-1111 out of Port B of Tester.

Result 1 is expected.

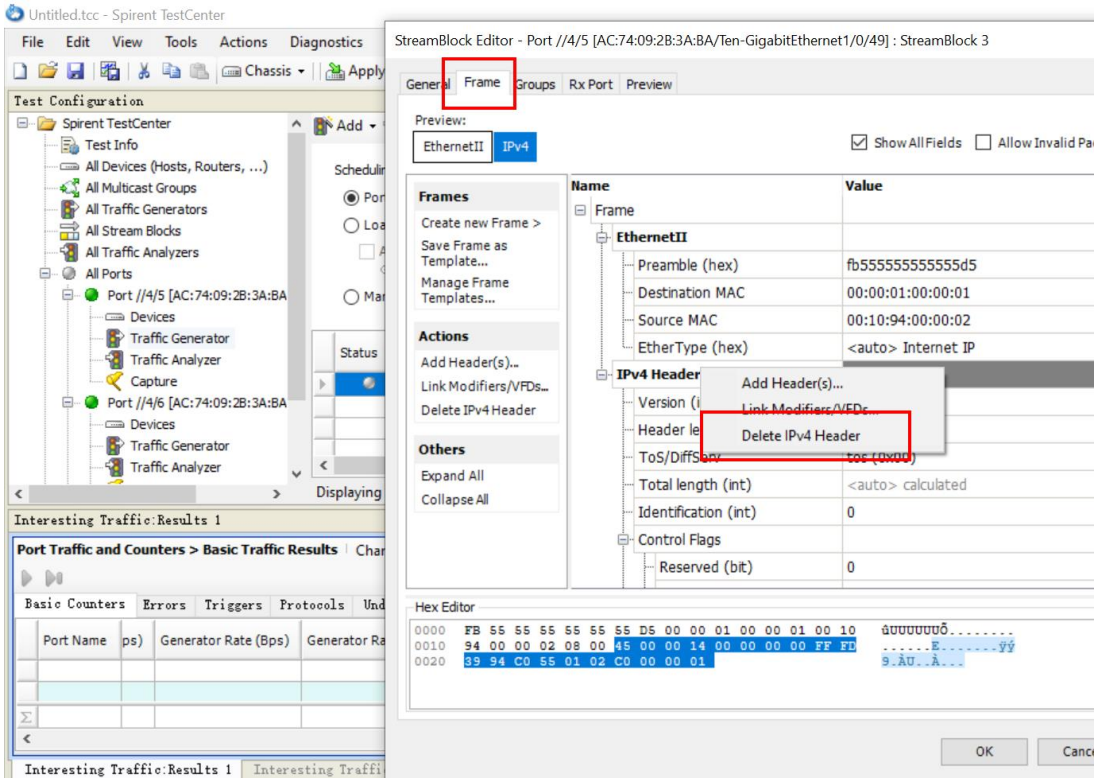
```
[DUT1]mac-address static 0-0-1111 interface Ten-GigabitEthernet 1/0/49 vlan 1
```

```
[DUT1]mac-address static 0-0-2222 interface Ten-GigabitEthernet 1/0/50 vlan 1
```

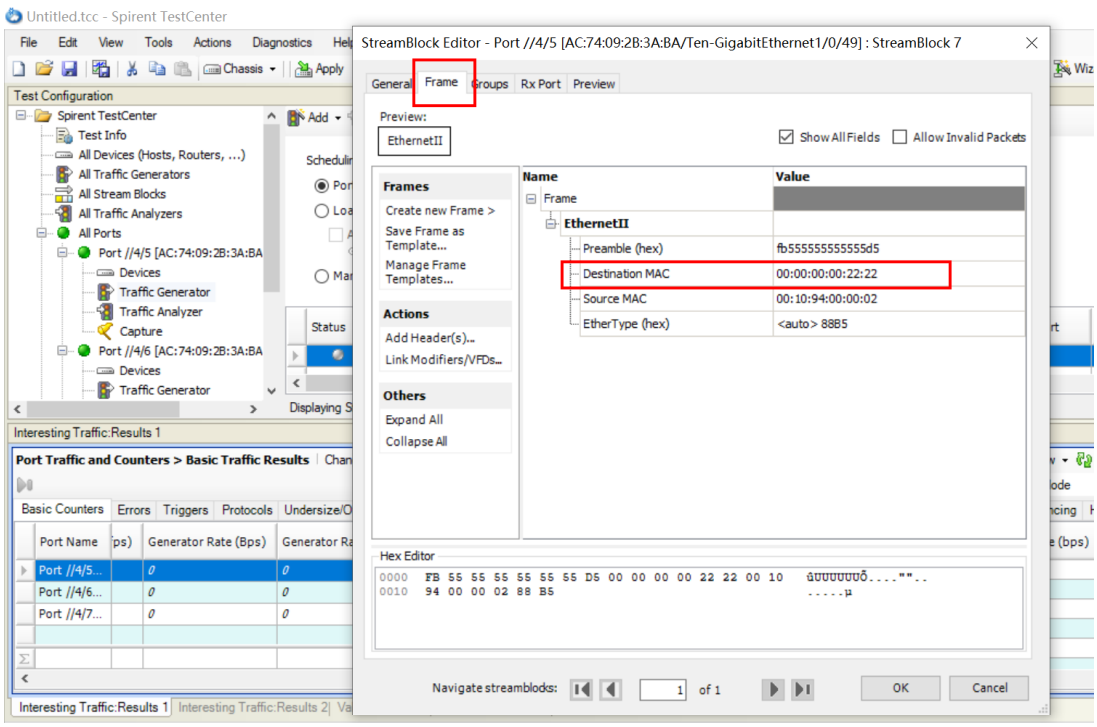
Create the traffic on Port A.
Add raw stream.



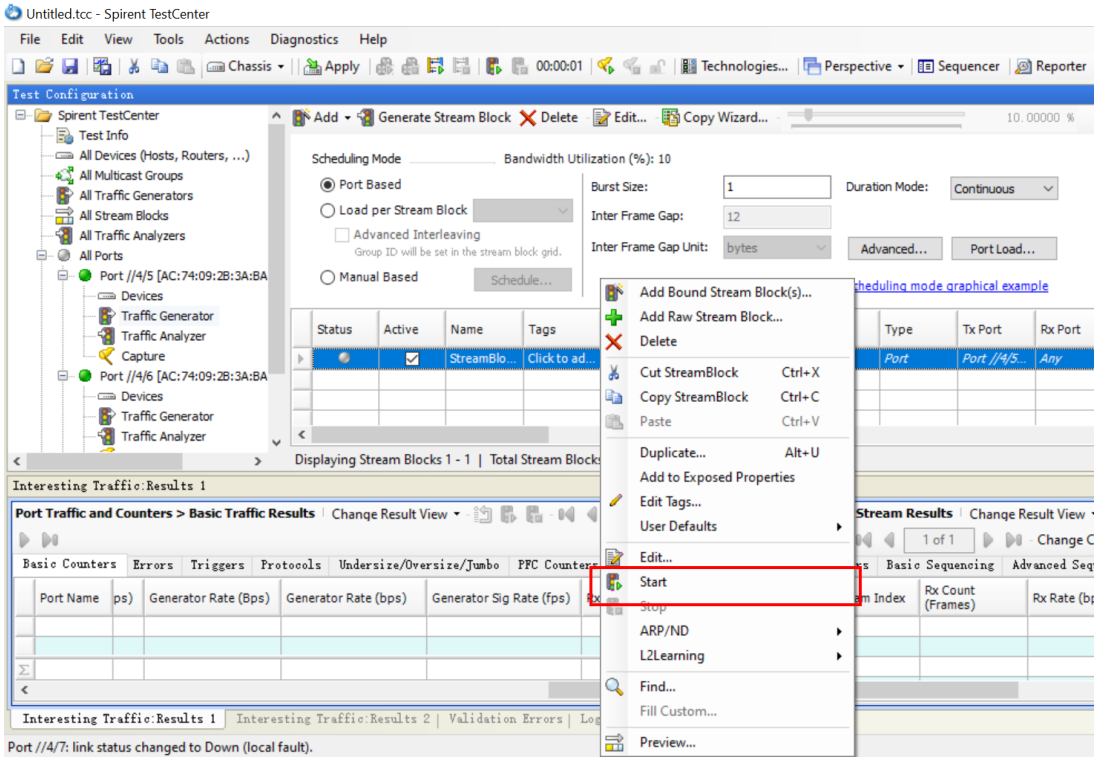
Delete the IPv4 header.



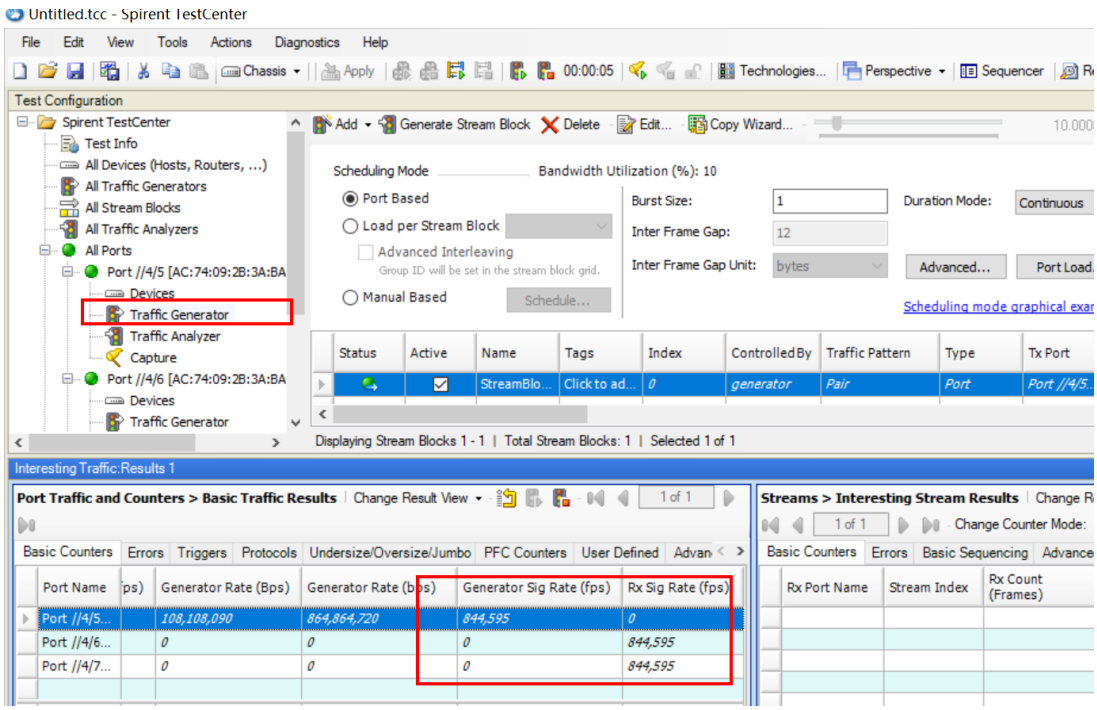
Change the destination MAC.



Send packets with destination MAC address 0-0-2222 out of Port A of Tester.

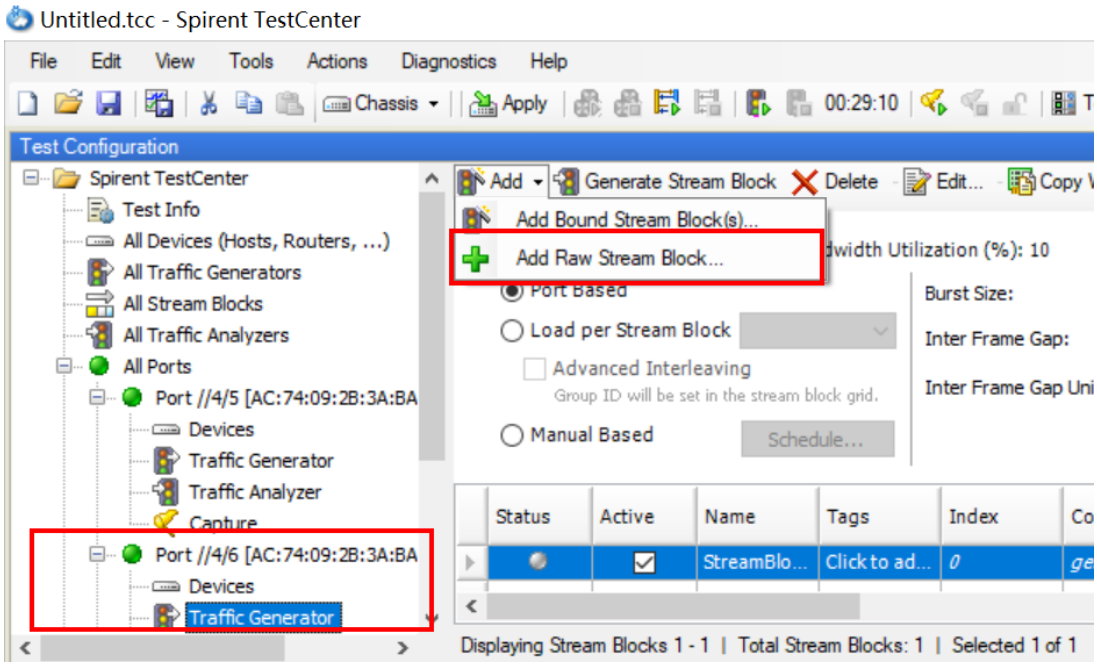


Packets sent out Port A of Tester are received on Port C of Tester.

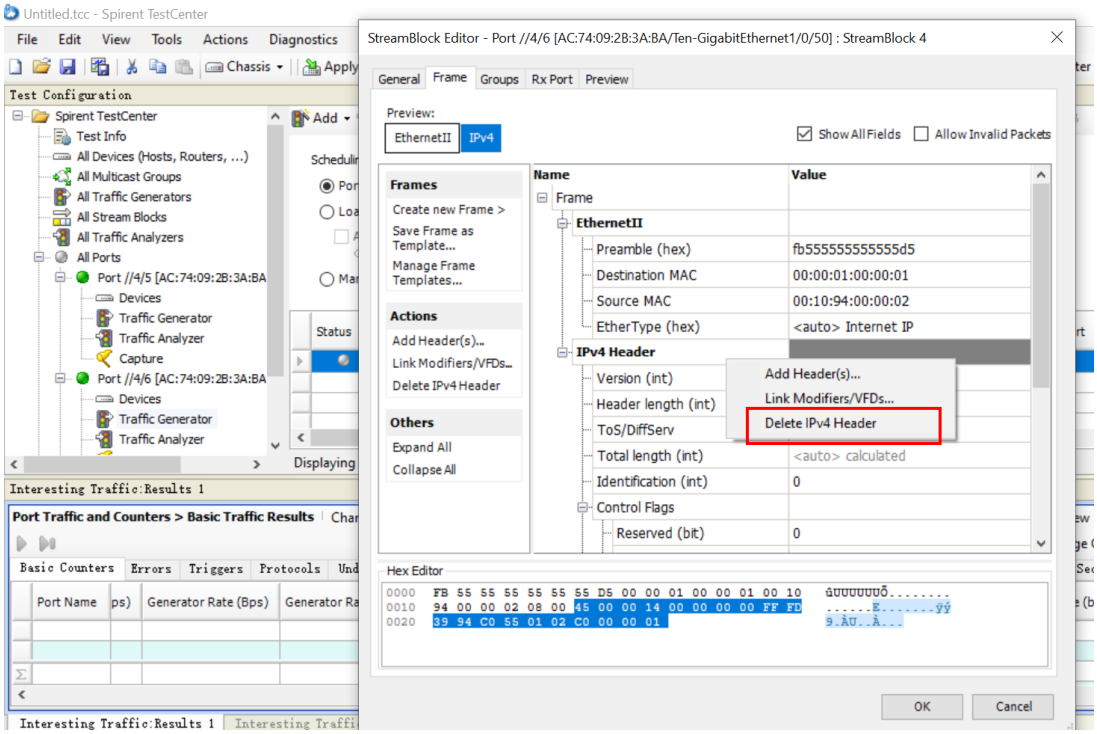


Create the traffic on Port B.

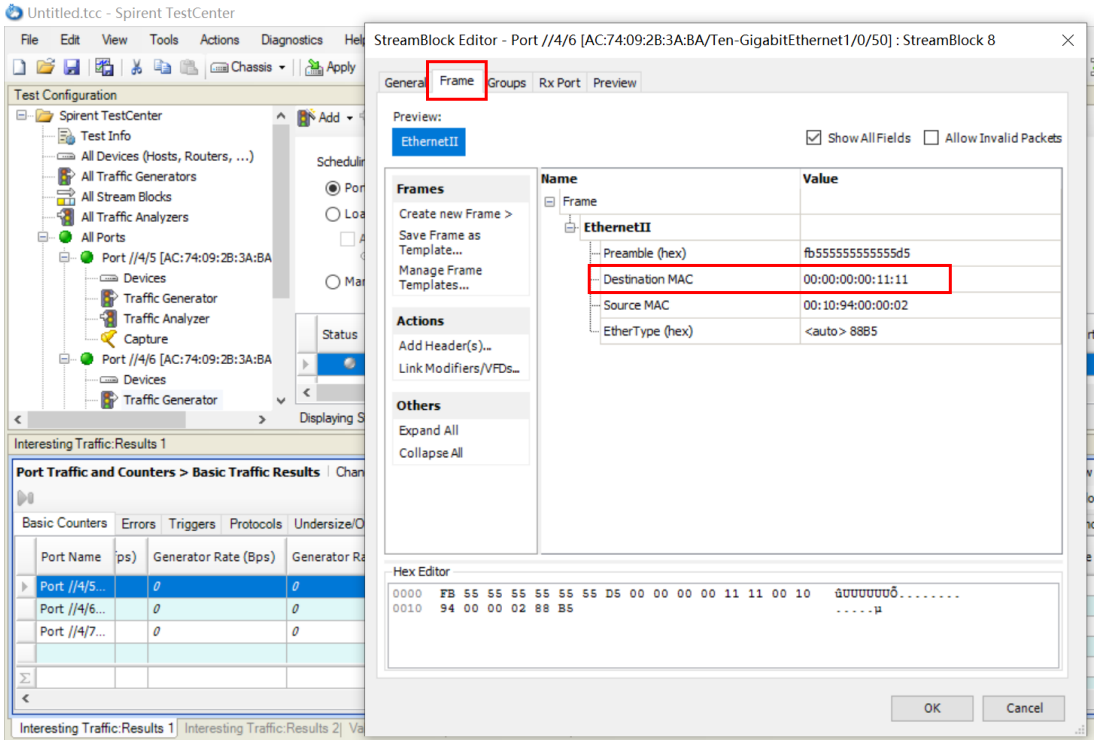
Add raw stream.



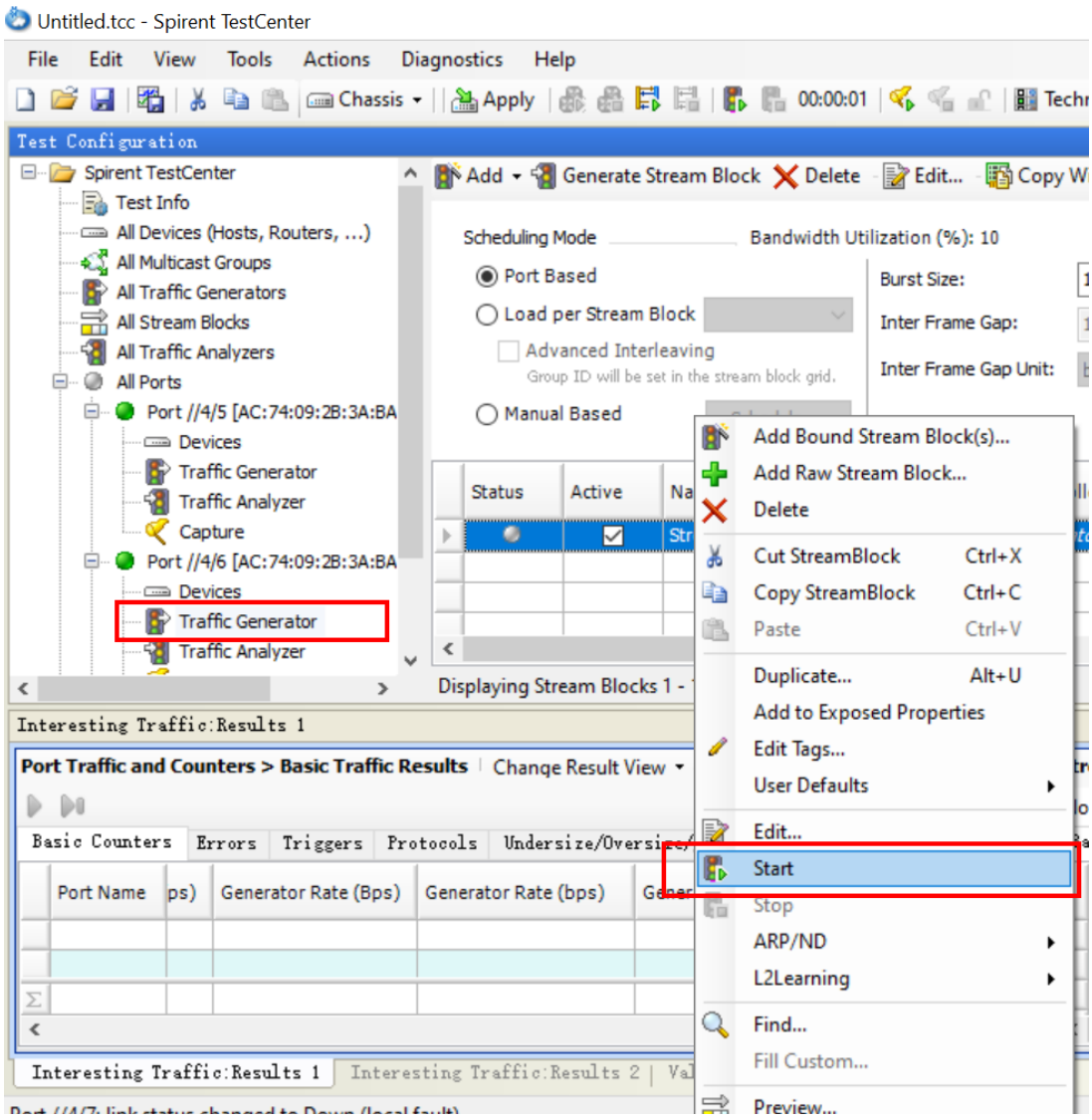
Delete the IPv4 header.



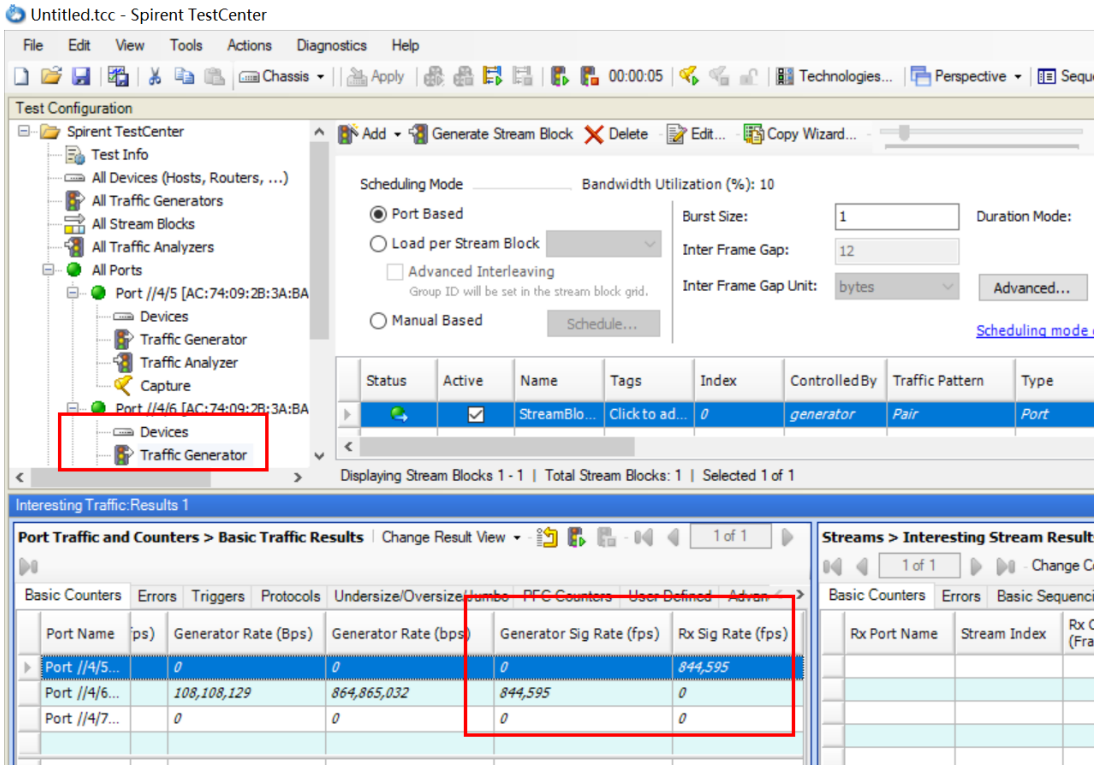
Change the destination MAC.



Send packets with destination MAC address 0-0-1111 out of Port B of Tester.



Port C cannot receive the packets.

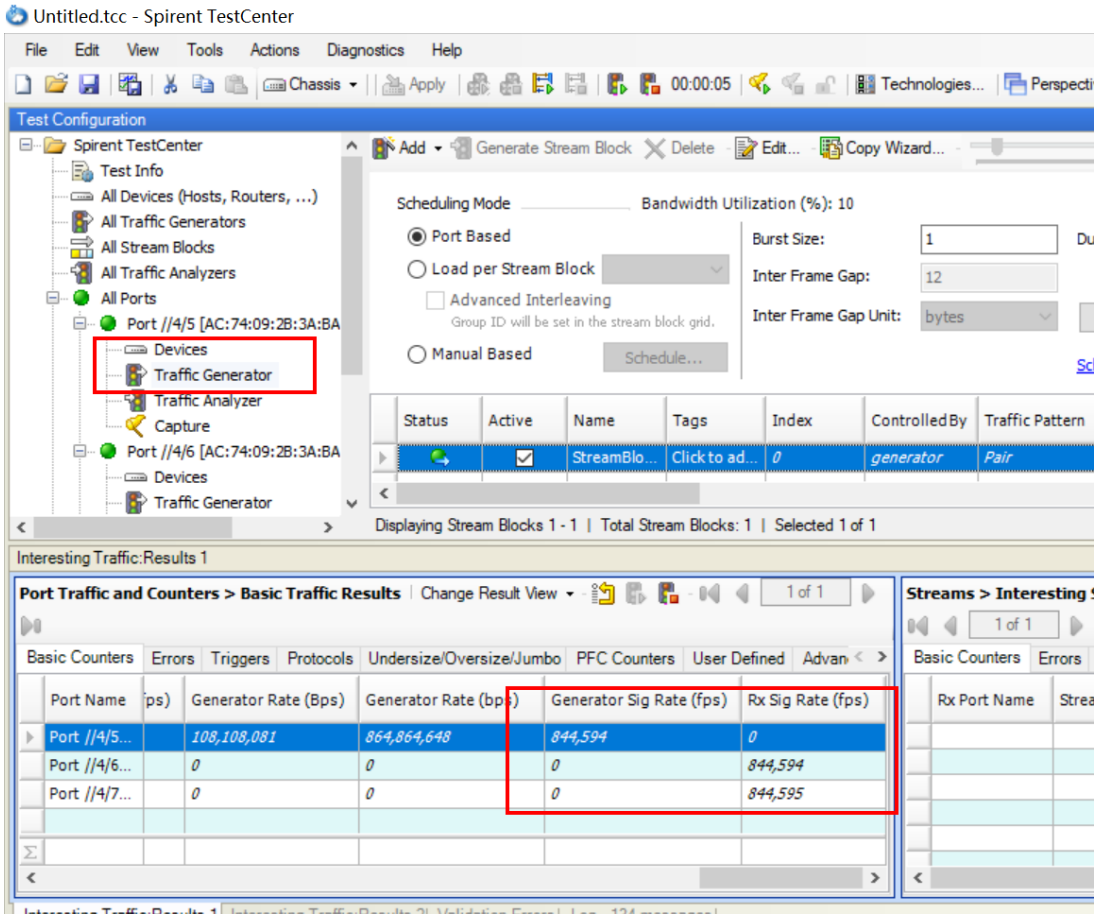


4. Configure mirroring group 1 to monitor bidirectional packets of Port 1. Send packets with destination MAC address 0-0-2222 out of Port A of Tester. Send packets with destination MAC address 0-0-1111 out of Port B of Tester. Result 2 is expected.

```
[DUT1]undo mirroring-group 1 mirroring-port Ten-GigabitEthernet 1/0/49
[DUT1]mirroring-group 1 mirroring-port Ten-GigabitEthernet 1/0/49 both
```

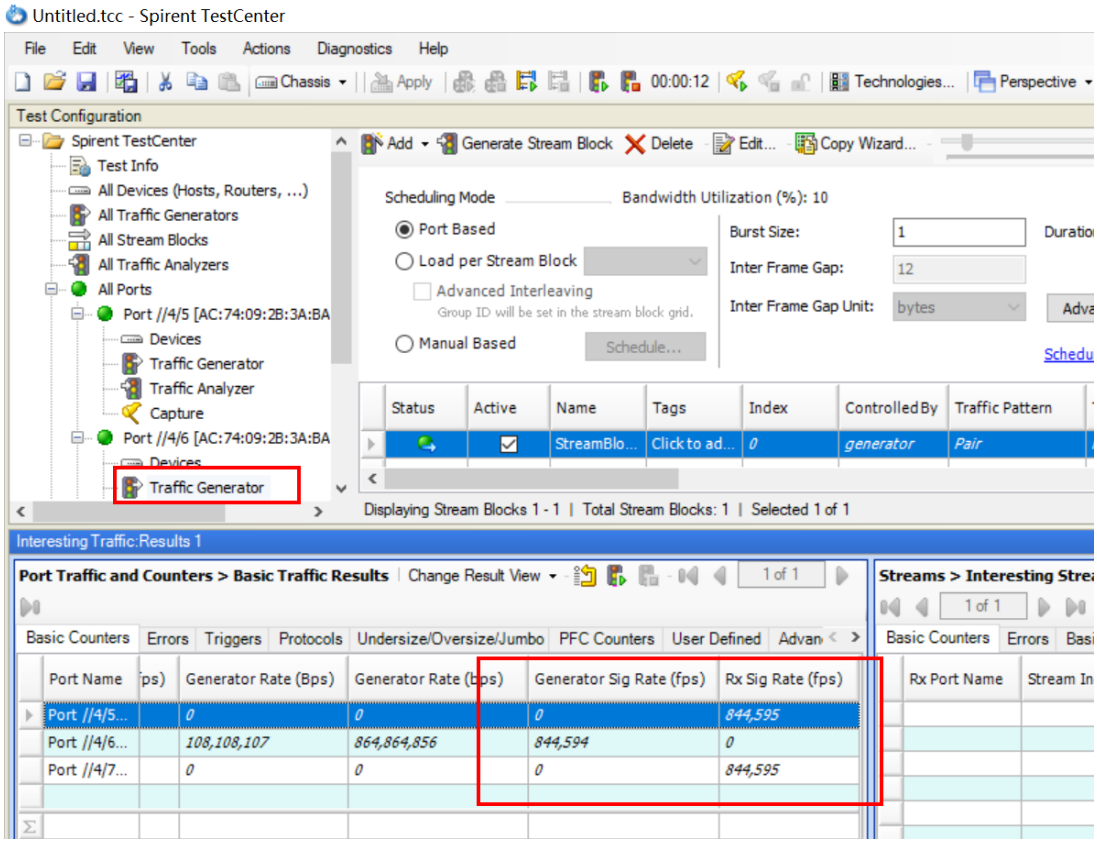
Send packets with destination MAC address 0-0-2222 out of Port A of Tester.

Packets sent out Port A of Tester are received on Port C of Tester.



Send packets with destination MAC address 0-0-1111 out of Port B of Tester.

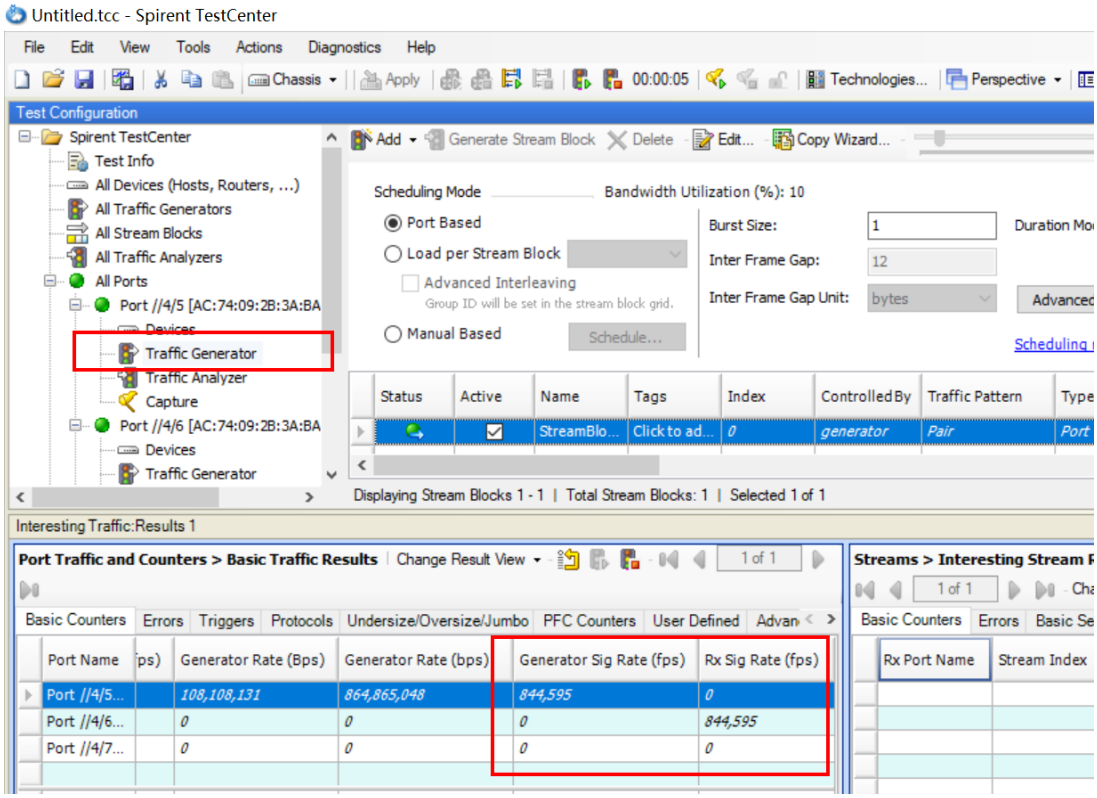
Packets sent out Port B of Tester are received on Port C of Tester.



5. Configure mirroring group 1 to monitor outbound packets of Port 1. Send packets with destination MAC address 0-0-2222 out of Port A of Tester. Send packets with destination MAC address 0-0-1111 out of Port B of Tester. Result 3 is expected.

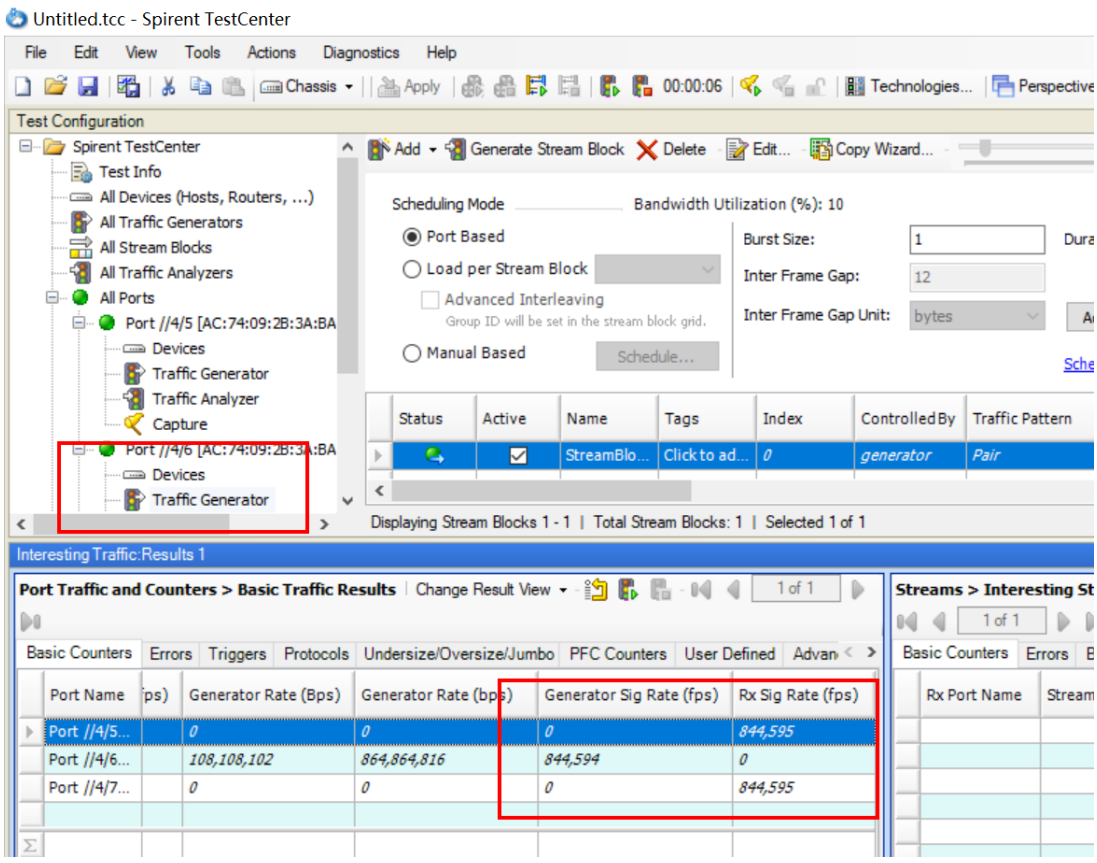
```
[DUT1]undo mirroring-group 1 mirroring-port Ten-GigabitEthernet 1/0/49
[DUT1]mirroring-group 1 mirroring-port Ten-GigabitEthernet 1/0/49 outbound
```

Send packets with destination MAC address 0-0-2222 out of Port A of Tester. Port C cannot receive the packets.



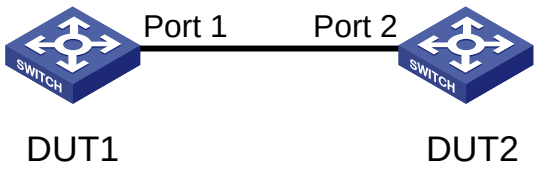
Send packets with destination MAC address 0-0-1111 out of Port B of Tester.

Packets sent out Port B of Tester are received on Port C of Tester.



☐ Passed	☐ Failed

2.8 LLDP

Test Item Name: LLDP
Work Hour: 20 min
Test Topology: 
Test Process: 1. Enable LLDP globally on DUT 1 and DUT 2. 2. Display the global local LLDP information on DUT 1. Result 1 is expected. 3. Display the local LLDP information about Port 1 on DUT 1. Result 2 is expected.

4. Display the LLDP information that Port 1 of DUT 1 has received from Port 2 of DUT 2. Result 3 is expected.

Expect Results:

1. The system displays the global local LLDP information on DUT 1, including the MAC address, device name, description, supported and enabled features of the system, hardware version, and firmware version.
2. The system displays the local LLDP information about Port 1 on DUT 1, including the port ID, management address, and port auto-negotiation configuration.
3. The system displays the LLDP information about Port 2 on DUT 2, including the port ID, management address, and port auto-negotiation configuration.

Actual Result:

1. Enable LLDP globally

lldp global enable

2. Display the LLDP neighbor information

```
[DUT]display lldp neighbor-information list
Chassis ID : * -- -- Nearest nontpmr bridge neighbor
             # -- -- Nearest customer bridge neighbor
             Default -- -- Nearest bridge neighbor
Local Interface Chassis ID      Port ID                 System Name
MGE0/0/0        000f-e219-4047  GigabitEthernet1/0/37   lab-lan-sw1
```

3. Display the LLDP local information

```
[DUT]display lldp local-information
Global LLDP local-information:
 Chassis ID          : fc60-9b96-a4cc
 System name         : DUT
 System description  :
   H3C Comware Platform Software, Software Version 7.1.070, Release 6515P06
   H3C S5560X-30C-PWR-EI
   Copyright (c) 2004-2020 New H3C Technologies Co., Ltd. All rights reserved.
 System capabilities supported : Bridge, Router, Customer Bridge, Service Bridge
 System capabilities enabled   : Bridge, Router, Customer Bridge

 MED information:
 Device class              : Connectivity device
 MED inventory information of master board:
 HardwareRev               : Ver.B
 FirmwareRev               : 117
 SoftwareRev               : 7.1.070 Release 6515P06
 SerialNum                 : 210235A1XE9204Q00002
 Manufacturer name         : H3C
 Model name                : H3C S5560X-30C-PWR-EI
 Asset tracking identifier  : Unknown
```

4. Display the LLDP neighbor information on interface

```
[DUT]display lldp neighbor-information interface M-GigabitEthernet 0/0/0
LLDP neighbor-information of port 631[M-GigabitEthernet0/0/0]:
LLDP agent nearest-bridge:
 LLDP neighbor index : 1
 ChassisID/subtype   : 000f-e219-4047/MAC address
 PortID/subtype      : GigabitEthernet1/0/37/Interface name
 Capabilities        : Bridge, Router
```

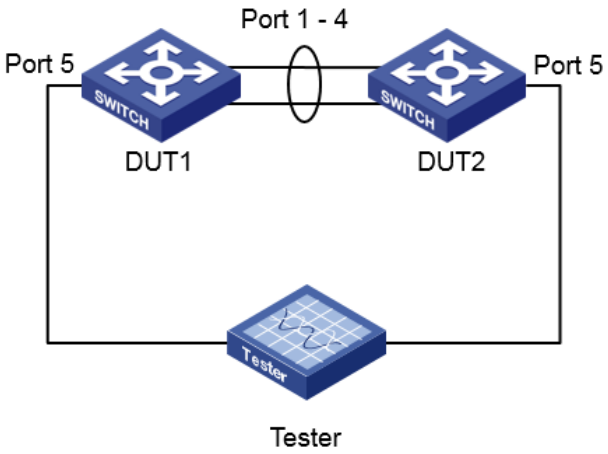
☐ Passed	☐ Failed

2.9 LACP (Link backup)

Test Item Name: LACP (Link backup)

Work Hour: 30 min

Test Topology:



Test Process:

1. On DUT 1 and DUT 2, create Layer 2 dynamic aggregate interface Bridge-Aggregation 1 and assign Layer 2 interfaces Port 1/2/3/4 to aggregation group 1.
2. On the tester, send a broadcast traffic flow out of Port A. Result 1 is expected.
3. Shut down a Selected port on a DUT.
4. On the tester, view traffic statistics about Port B. Result 2 is expected.
5. Bring up the down port.
6. On the tester, view traffic statistics about Port B. Result 2 is expected.

Expect Results:

1. Port B receives the broadcast traffic sent by Port A.
2. Transient traffic loss occurs, and then Port B receives the broadcast traffic sent by Port A.

Actual Result：

1. Create aggregation group 1 with dynamic mode and add 4 ports

#

interface Bridge-Aggregation1

link-aggregation mode dynamic

#

#

interface Ten-GigabitEthernet1/0/49

port link-mode bridge

port link-aggregation group 1

#

interface Ten-GigabitEthernet1/0/50

port link-mode bridge

port link-aggregation group 1

#

interface Ten-GigabitEthernet1/0/51

port link-mode bridge

port link-aggregation group 1

#

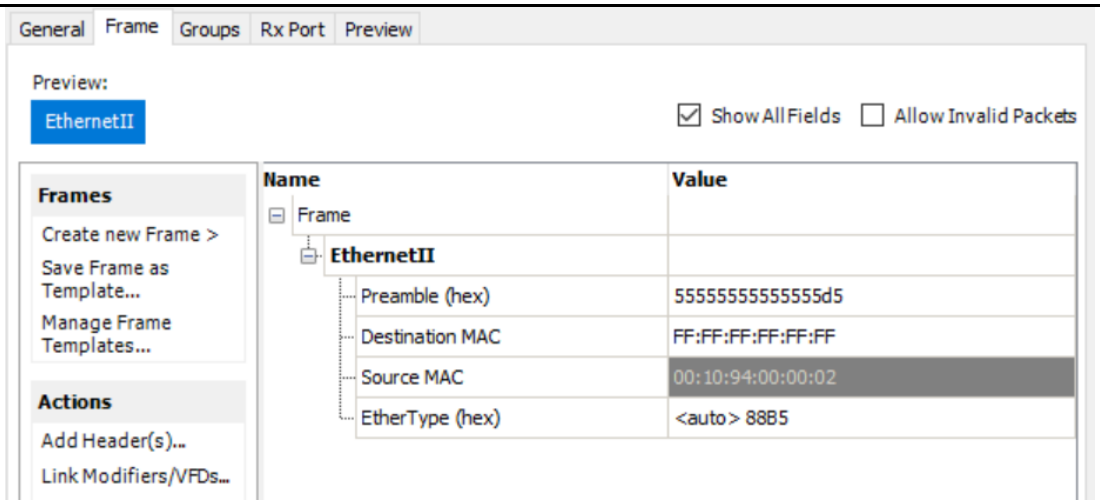
interface Ten-GigabitEthernet1/0/52

port link-mode bridge

port link-aggregation group 1

#

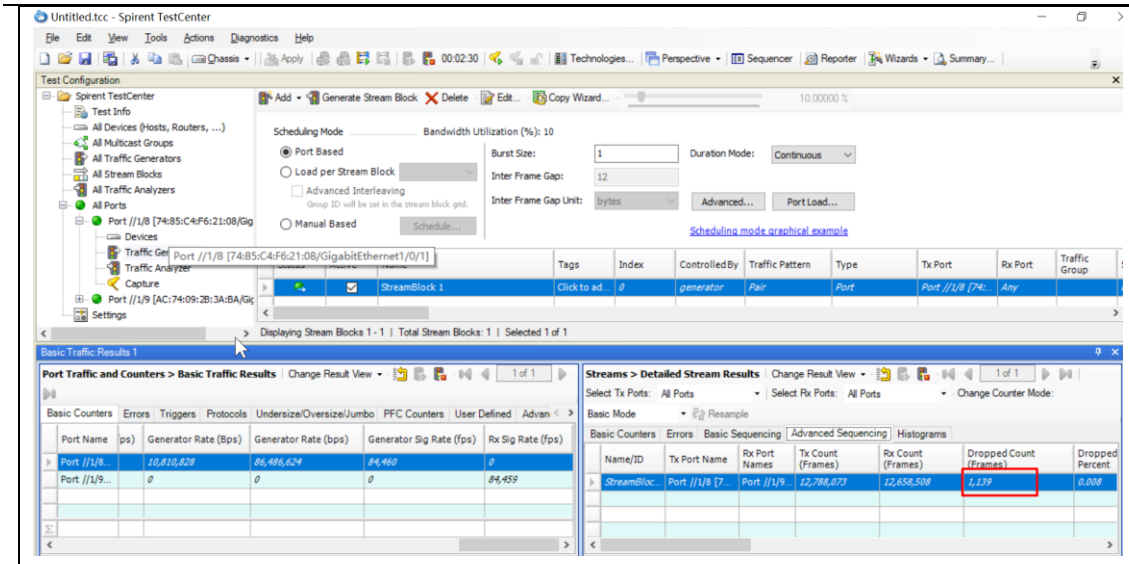
2. Send traffic on Port A



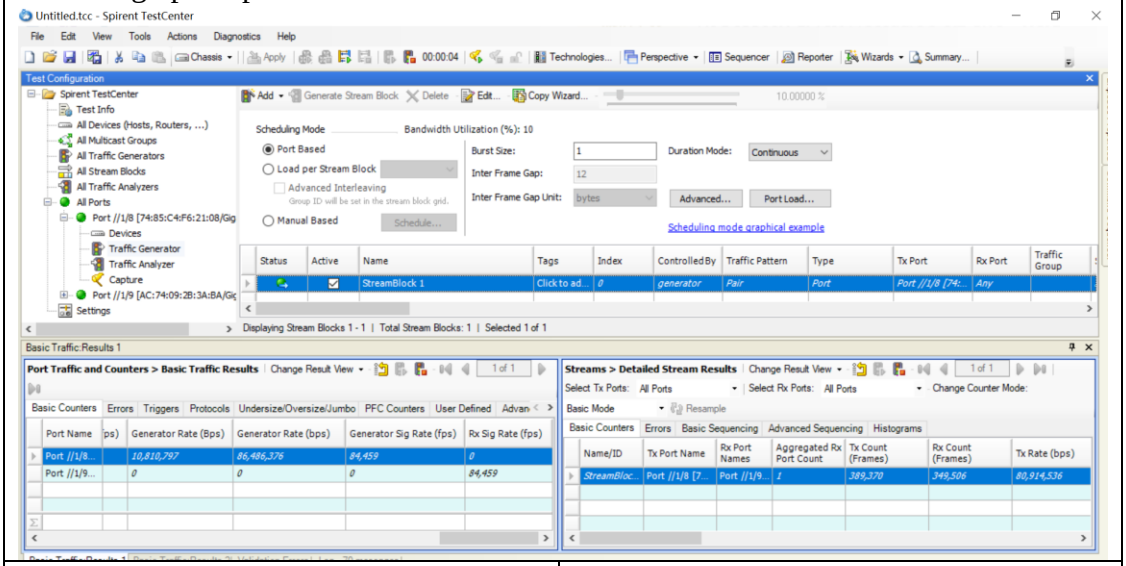
3. Shutdown 1 member port and check the traffic loss

```
Management VLANs: None
System ID: 0x8000, 7485-c4f6-2108
Local:
  Port                Status   Priority Index    Oper-Key               Flag
  XGE1/0/25(R)        S        32768    1        1                      {ACDEF}
  XGE1/0/26           S        32768    2        1                      {ACDEF}
  XGE1/0/27           S        32768    3        1                      {ACDEF}
  XGE1/0/28           S        32768    4        1                      {ACDEF}
Remote:
  Actor               Priority Index    Oper-Key SystemID               Flag
  XGE1/0/25           32768    1        1        0x8000, ac74-092b-3aba {ACDEF}
  XGE1/0/26           32768    2        1        0x8000, ac74-092b-3aba {ACDEF}
  XGE1/0/27           32768    3        1        0x8000, ac74-092b-3aba {ACDEF}
  XGE1/0/28           32768    4        1        0x8000, ac74-092b-3aba {ACDEF}
[5560x-ei-1]
```

```
[5560x-ei-1]int te 1/0/25
[5560x-ei-1-Ten-GigabitEthernet1/0/25]shu
%Jan 29 06:25:39:475 2021 5560x-ei-1 LAGG/6/LAGG_INACTIVE_PHYSTATE: Member port XGE1/0/25 of agg
regation group BAGG1 changed to the inactive state, because the physical or line protocol state
of the port was down.
%Jan 29 06:25:39:512 2021 5560x-ei-1 IFNET/3/PHY_UPDOWN: Physical state on the interface Ten-Gig
abitEthernet1/0/25 changed to down.
%Jan 29 06:25:39:519 2021 5560x-ei-1 IFNET/5/LINK_UPDOWN: Line protocol state on the interface T
en-GigabitEthernet1/0/25 changed to down.
[5560x-ei-1-Ten-GigabitEthernet1/0/25]
```



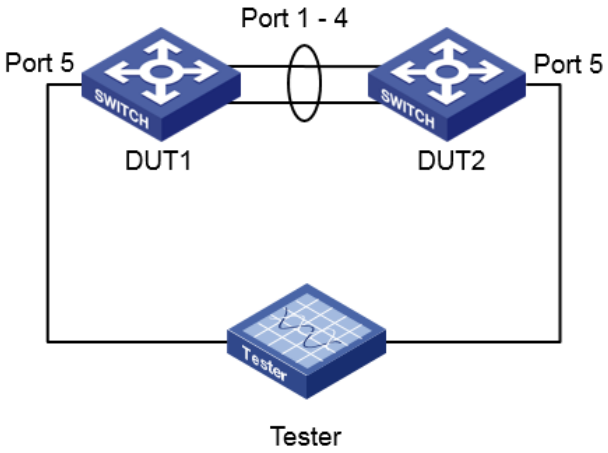
4. Bring up the port and see the traffic can recover



☐ Passed	☐ Failed

2.10 LACP (Load sharing)

Test Item Name: LACP (Load sharing)
Work Hour: 30 min
Test Topology:



Test Process:

1. Clear interface packet statistics on DUT 1.
2. On the tester, send Layer 2 broadcast packets sourced from 200 consecutive MAC addresses out of Port A. Result 1 is expected.
3. On DUT 1 and DUT 2, create VLAN-interface 1 and assign the VLAN interfaces IP addresses that belong to the same subnet.
4. On DUT 1, create VLAN 2 and assign Port 5 to VLAN 2. Create VLAN-interface 2 and assign it an IP address.
5. On the tester, send Layer 3 packets out of Port A. The packets are destined for VLAN-interface 1 on DUT 2 and sourced from 200 consecutive IP addresses in the same subnet as the IP address of VLAN-interface 2 on DUT 1. Result 1 is expected.

Expect Results:

1. On DUT 1, the traffic is distributed to Port 1/2/3/4 almost evenly.

Actual Result：

1. Create aggregation group 1 with dynamic mode and add 4 ports

#

interface Bridge-Aggregation1

link-aggregation mode dynamic

#

#

interface Ten-GigabitEthernet1/0/49

port link-mode bridge

port link-aggregation group 1

#

interface Ten-GigabitEthernet1/0/50

port link-mode bridge

port link-aggregation group 1

#

interface Ten-GigabitEthernet1/0/51

port link-mode bridge

port link-aggregation group 1

#

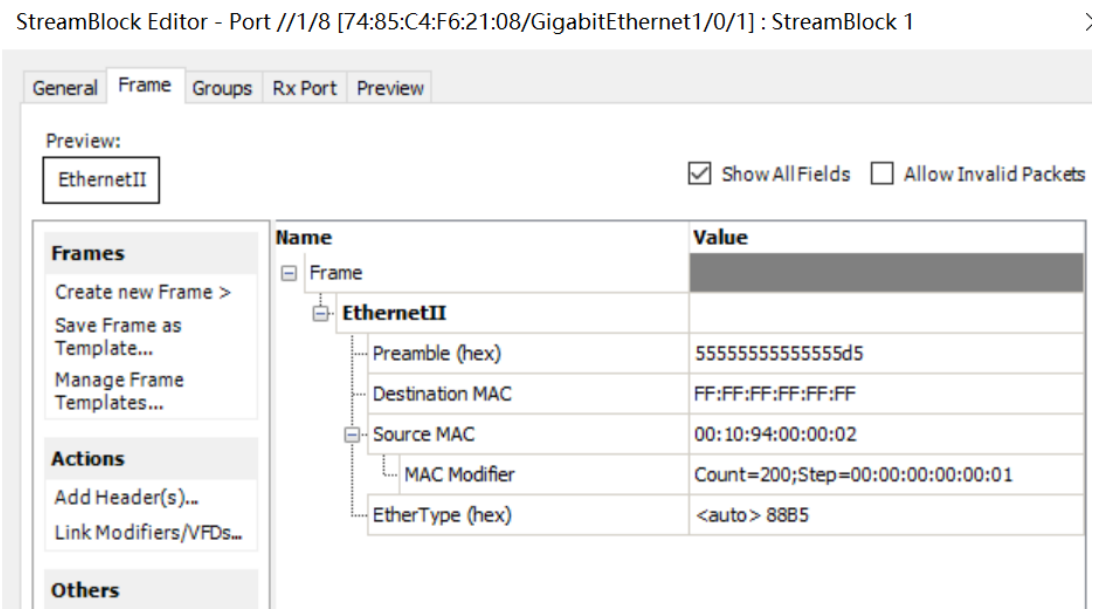
interface Ten-GigabitEthernet1/0/52

port link-mode bridge

port link-aggregation group 1

#

2. Send traffic with changing source mac



3. On DUT 1, the traffic is distributed to Port 1/2/3/4 almost evenly.

```
[5560x-ei-1-GigabitEthernet1/0/1]d c r i i
Usage: Bandwidth utilization in percentage
Interface            Usage (%)    Total (pps)   Broadcast (pps)   Multicast (pps)
BAGG1                        0              0                --                --
GE1/0/1                     10          84458                --                --
XGE1/0/25                    0              0                --                --
XGE1/0/26                    0              0                --                --
XGE1/0/27                    0              0                --                --
XGE1/0/28                    0              0                --                --

 Overflow: More than 14 digits.
       --: Not supported.
[5560x-ei-1-GigabitEthernet1/0/1]d c r o i
Usage: Bandwidth utilization in percentage
Interface            Usage (%)    Total (pps)   Broadcast (pps)   Multicast (pps)
BAGG1                        0          84456                --                --
GE1/0/1                      0              0                --                --
XGE1/0/25                    0          21114                --                --
XGE1/0/26                    0          21114                --                --
XGE1/0/27                    0          21114                --                --
XGE1/0/28                    0          21114                --                --

 Overflow: More than 14 digits.
       --: Not supported.
```

4. Configure VLAN-int on DUT

DUT1

#

interface Vlan-interface1

ip address 10.1.1.1 255.255.255.0

#

DUT2

#

interface Vlan-interface1

ip address 10.1.1.2 255.255.255.0

#

5. Configure VLAN-int 2 on DUT1

#

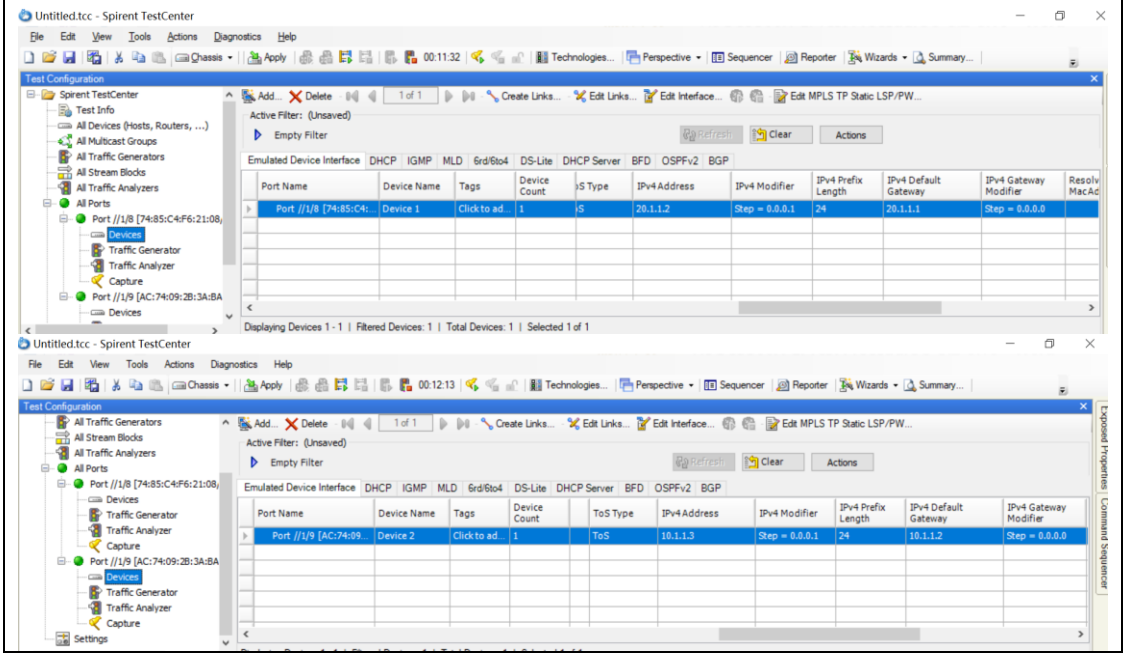
interface Vlan-interface2

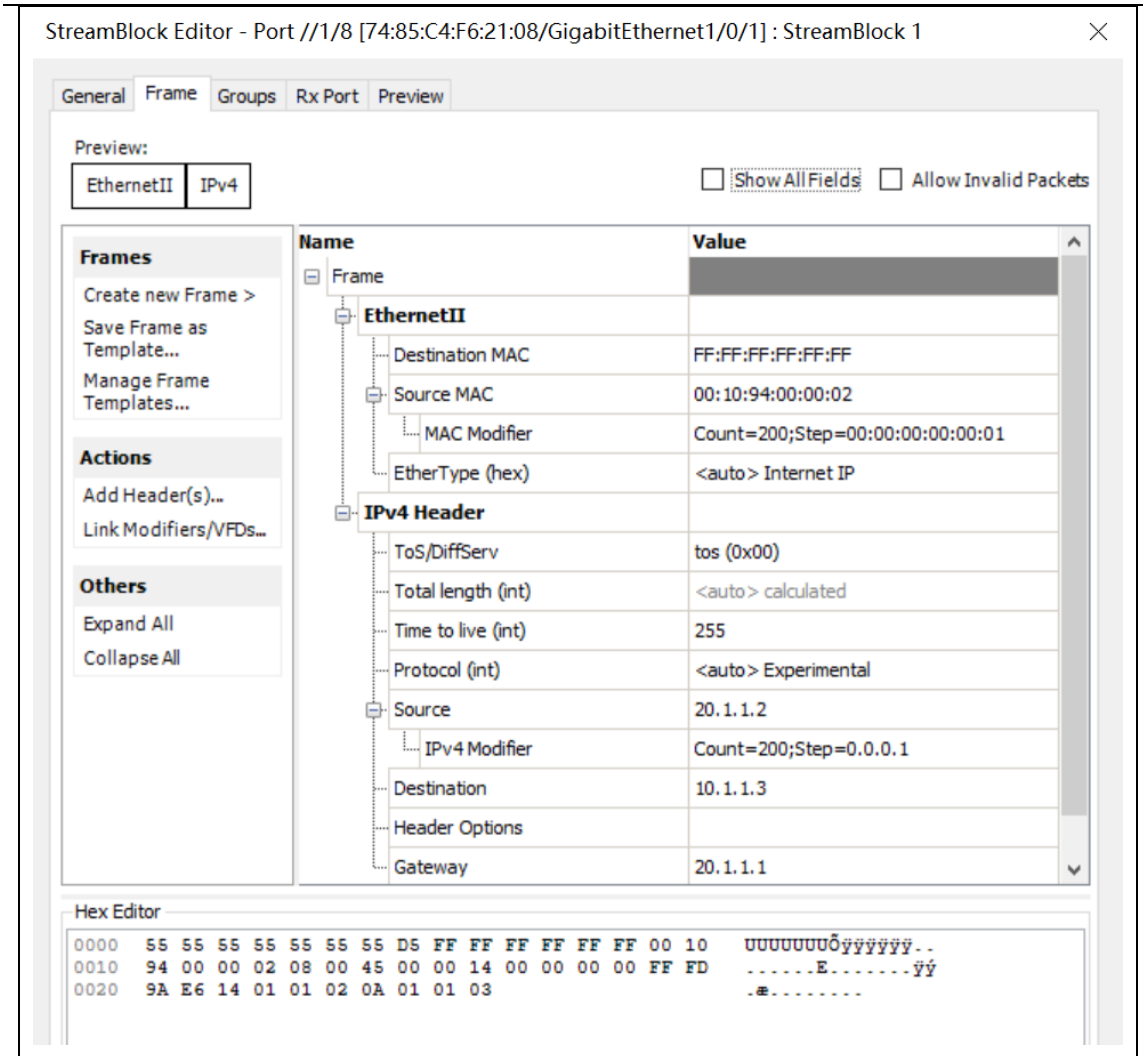
ip address 20.1.1.1 255.255.255.0

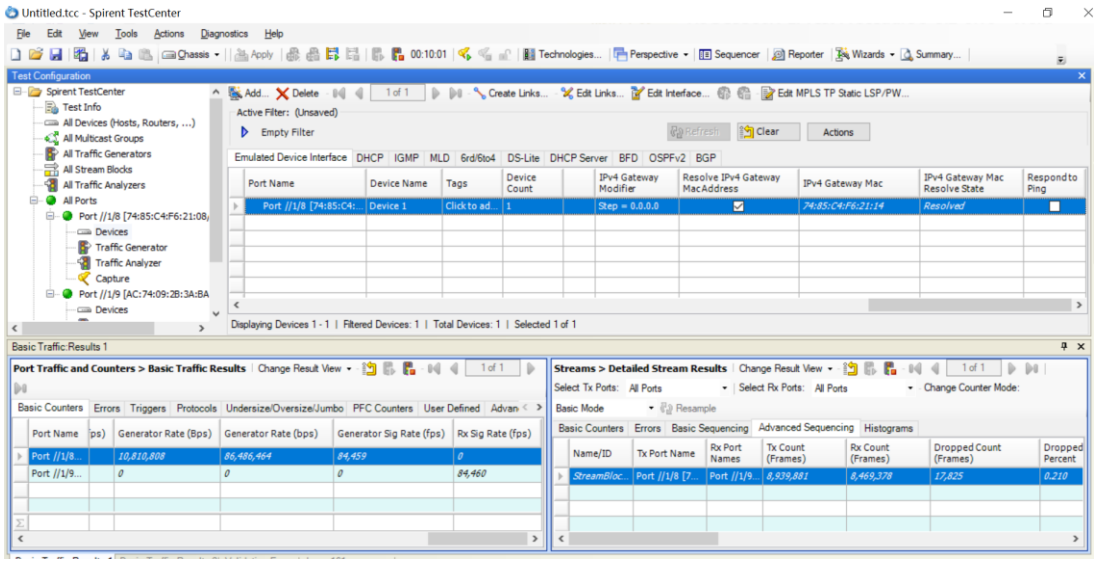
#

6. On the tester, send Layer 3 packets out of Port A. The packets are destined for VLAN-interface 1 on DUT 2 and sourced from 200 consecutive IP addresses in

the same subnet as the IP address of VLAN-interface 2 on DUT 1. Result 1 is expected.




StreamBlock Editor - Port //1/8 [74:85:C4:F6:21:08/GigabitEthernet1/0/1] : StreamBlock 1
General
Frame
Groups
Rx Port
Preview
Preview:
EthernetII
IPv4
Show All Fields
Allow Invalid Packets
Frames
Create new Frame >
Save Frame as Template...
Manage Frame Templates...
Actions
Add Header(s)...
Link Modifiers/VFDs...
Others
Expand All
Collapse All
Name
Value
Frame
EthernetII
Destination MAC
FF:FF:FF:FF:FF:FF
Source MAC
00:10:94:00:00:02
MAC Modifier
Count=200;Step=00:00:00:00:00:01
EtherType (hex)
<auto> Internet IP
IPv4 Header
ToS/DiffServ
tos (0x00)
Total length (int)
<auto> calculated
Time to live (int)
255
Protocol (int)
<auto> Experimental
Source
20.1.1.2
IPv4 Modifier
Count=200;Step=0.0.0.1
Destination
10.1.1.3
Header Options
Gateway
20.1.1.1
Hex Editor
0000 55 55 55 55 55 55 55 D5 FF FF FF FF FF FF 00 10
0010 94 00 00 02 08 00 45 00 00 14 00 00 00 00 FF FD
0020 9A E6 14 01 01 02 0A 01 01 03


Untitled.tcc - Spirent TestCenter
Test Configuration
Basic Traffic Results 1
Port Traffic and Counters > Basic Traffic Results
Streams > Detailed Stream Results

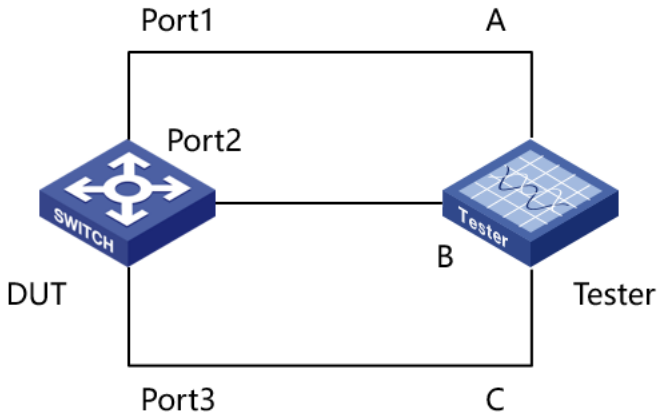
☐ Passed	☐ Failed

2.11 Dynamic MAC limit

Test Item Name: Dynamic MAC limit

Work Hour：30 min

Test Topology:



Test Process:

1. On the DUT, set the MAC learning limit to 100 on Port 1.
2. On the tester, send untagged broadcast packets through Port A. The source MAC addresses of the packets are 1000 consecutive MAC addresses starting at 0-0-1111. Result 1 is expected.
3. On the DUT, set the MAC learning limit to 150 on Port 3.
4. On the tester, send untagged broadcast packets through Port C. The source MAC addresses of the packets are 1000 consecutive MAC addresses starting at 0-0-1111. Result 2 is expected.

Expect Results:

1. The DUT has learned 100 MAC addresses on Port 1.
2. The DUT has learned 150 MAC addresses on Port 3.

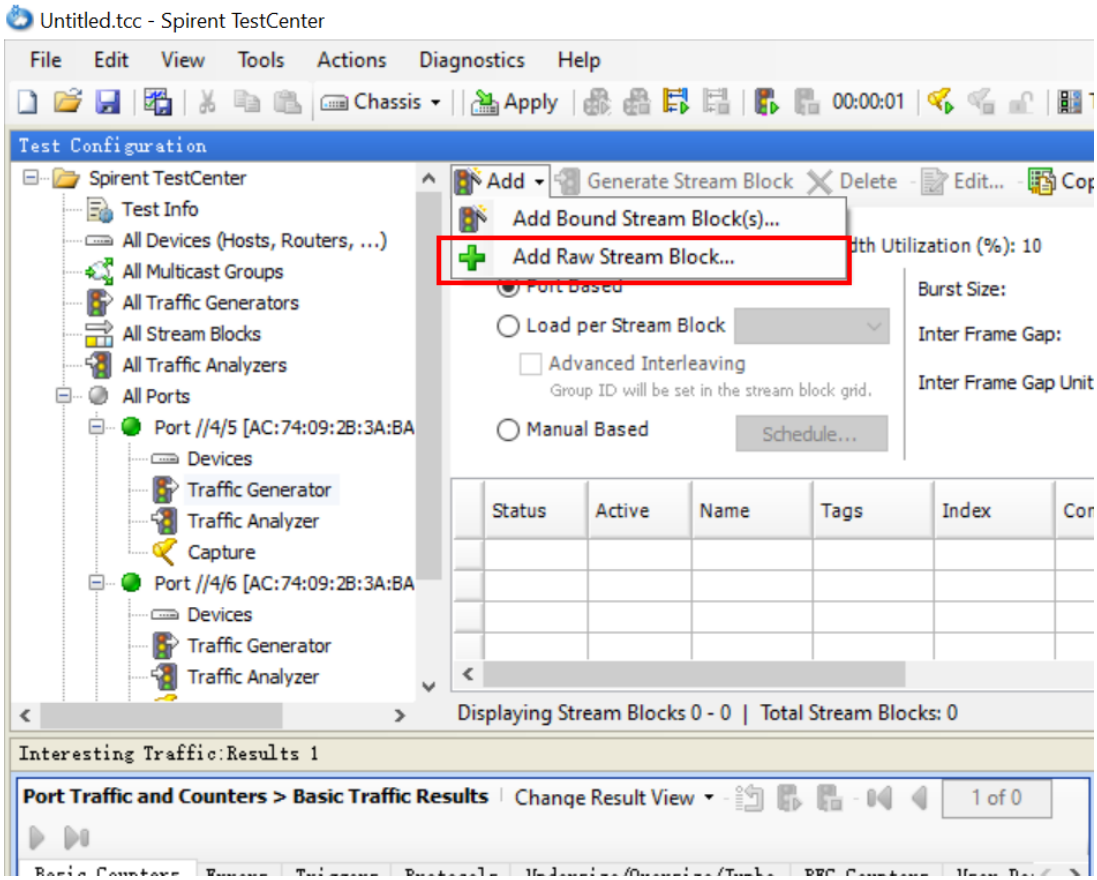
Actual Result：

1. On the DUT, set the MAC learning limit to 100 on Port 1.

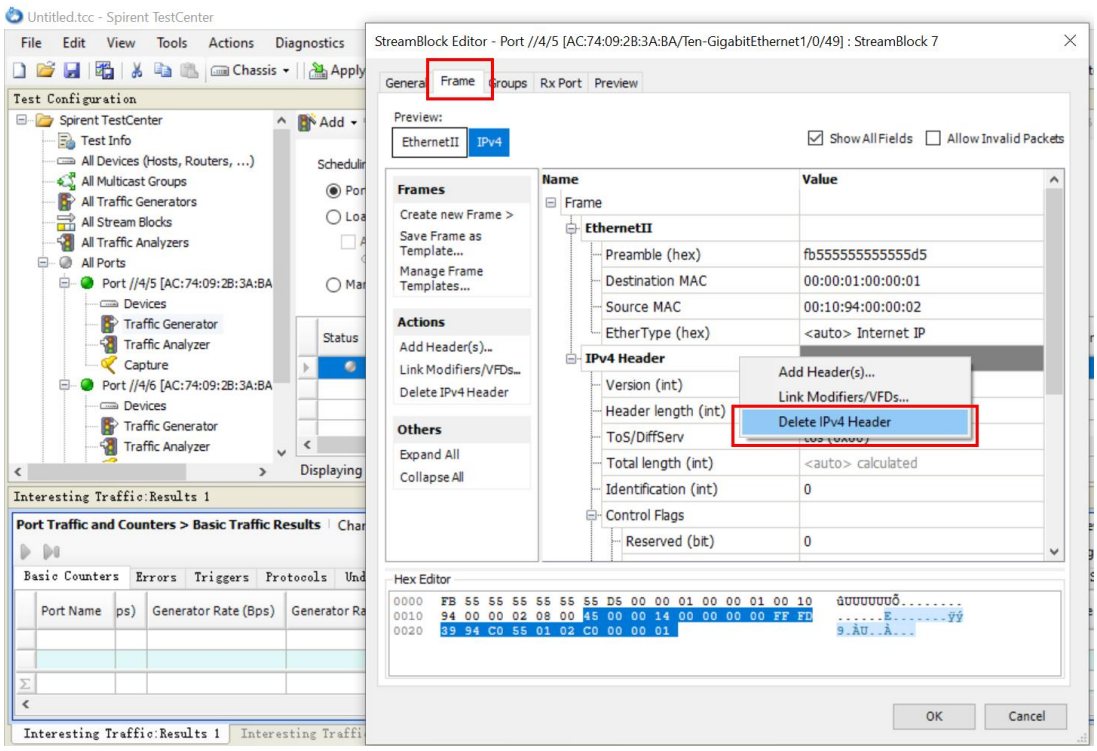
```
[DUT]interface Ten-GigabitEthernet1/0/49
[DUT-Ten-GigabitEthernet1/0/49]mac-address max-mac-count 100
```

2. On the tester, send untagged broadcast packets through Port A. The source MAC addresses of the packets are 1000 consecutive MAC addresses starting at 0-0-1111. Result 1 is expected.

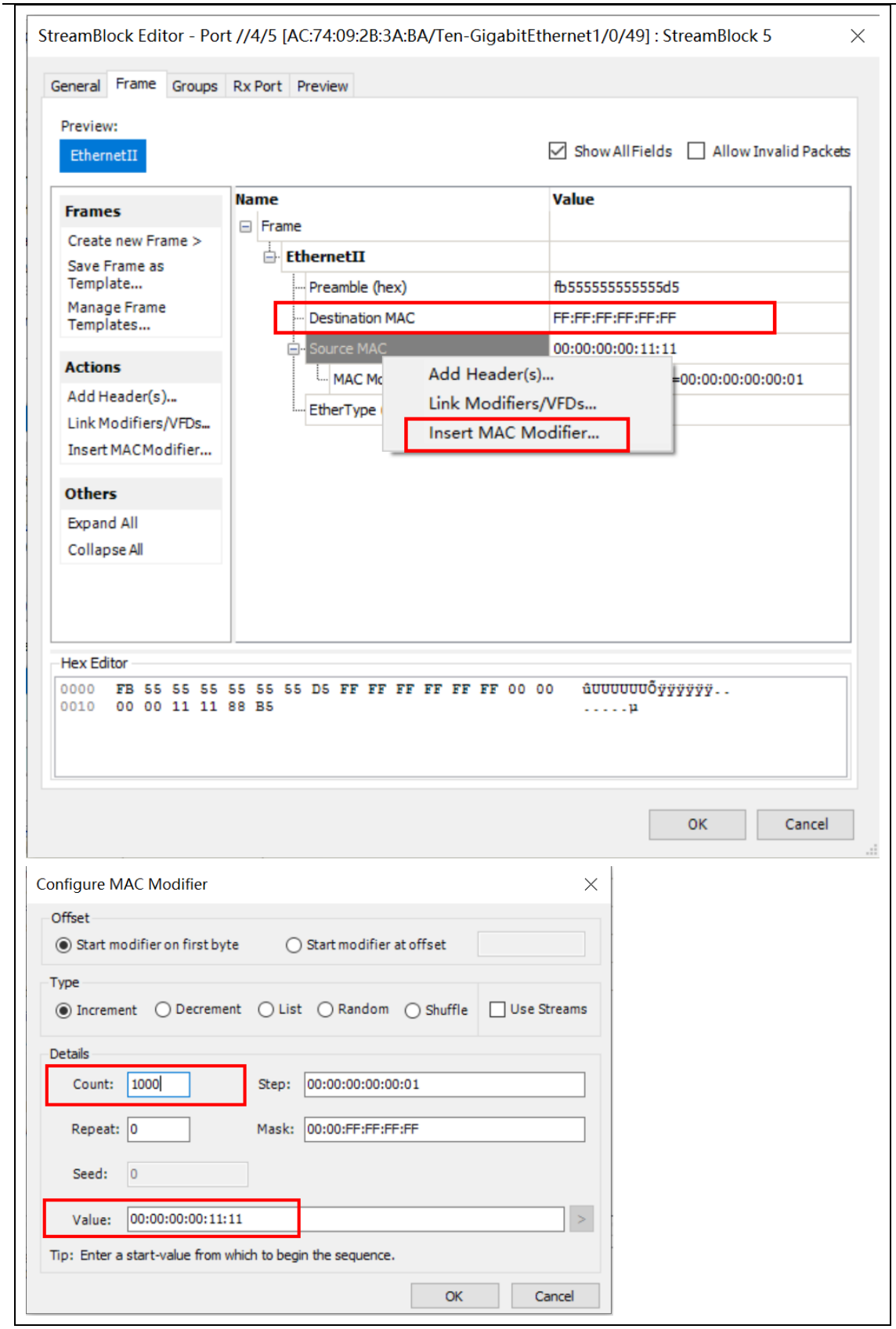
Add raw traffic.



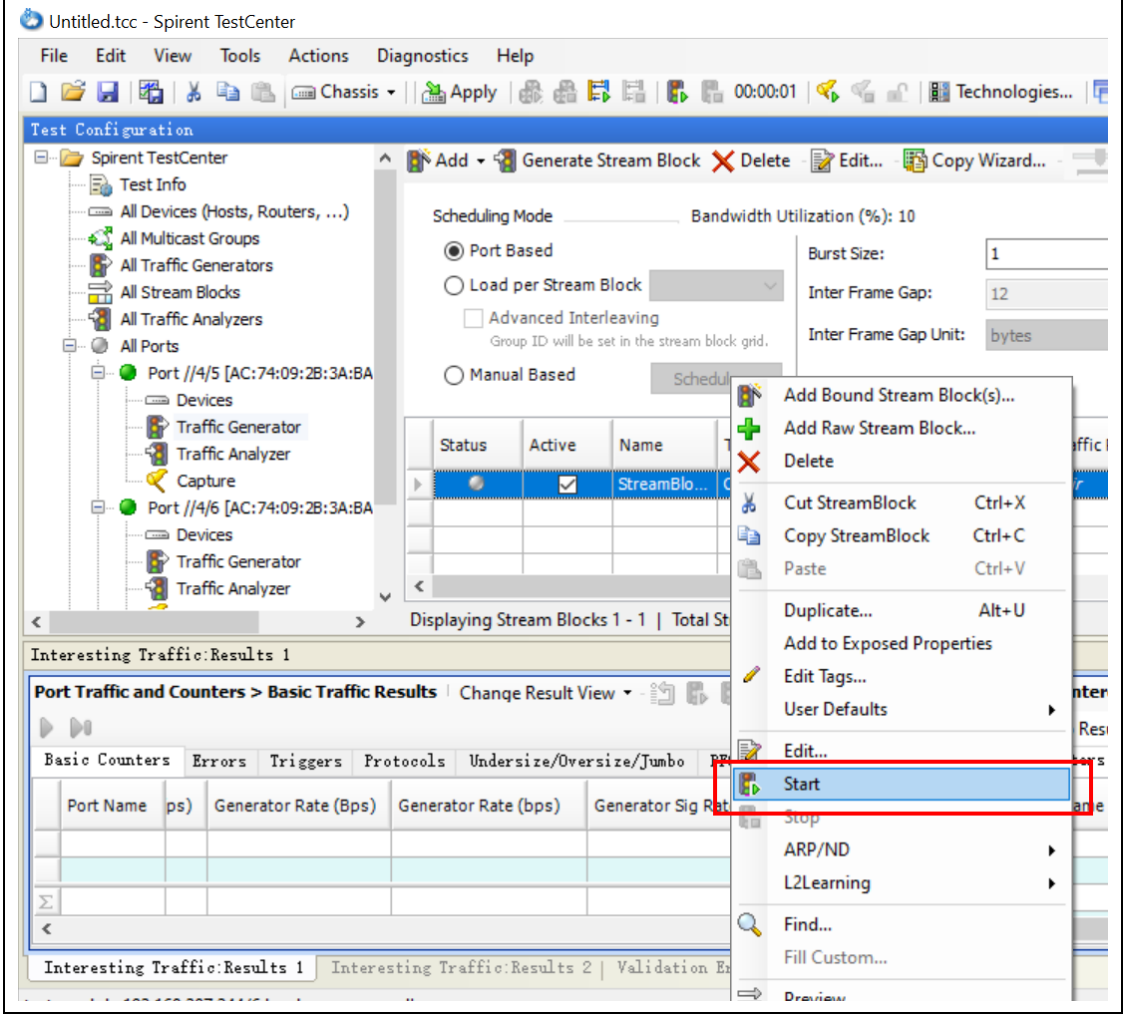
Delete the IPv4 header.

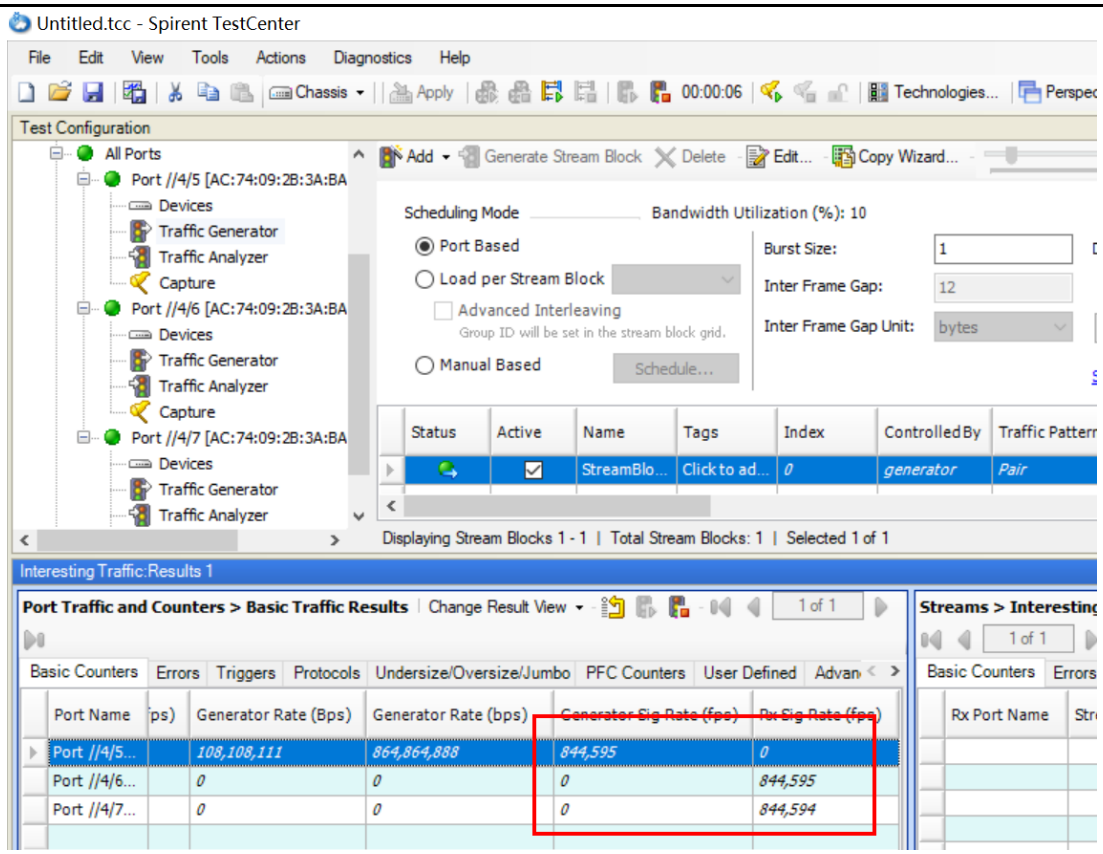


Change the source MAC modifier.


StreamBlock Editor - Port //4/5 [AC:74:09:2B:3A:BA/Ten-GigabitEthernet1/0/49] : StreamBlock 5
General
Frame
Groups
Rx Port
Preview
Preview:
EthernetII
Show All Fields
Allow Invalid Packets
Frames
Create new Frame >
Save Frame as Template...
Manage Frame Templates...
Actions
Add Header(s)...
Link Modifiers/VFDs...
Insert MAC Modifier...
Others
Expand All
Collapse All
Name
Value
Frame
EthernetII
Preamble (hex)
fb555555555555d5
Destination MAC
FF:FF:FF:FF:FF:FF
Source MAC
00:00:00:00:11:11
MAC Mc
=00:00:00:00:00:01
EtherType
Add Header(s)...
Link Modifiers/VFDs...
Insert MAC Modifier...
Hex Editor
0000 FB 55 55 55 55 55 55 D5 FF FF FF FF FF FF 00 00
0010 00 00 11 11 88 B5
OK
Cancel
Configure MAC Modifier
Offset
Start modifier on first byte
Start modifier at offset
Type
Increment
Decrement
List
Random
Shuffle
Use Streams
Details
Count: 1000
Step: 00:00:00:00:00:01
Repeat: 0
Mask: 00:00:FF:FF:FF:FF
Seed: 0
Value: 00:00:00:00:11:11
Tip: Enter a start-value from which to begin the sequence.
OK
Cancel

Send the traffic.





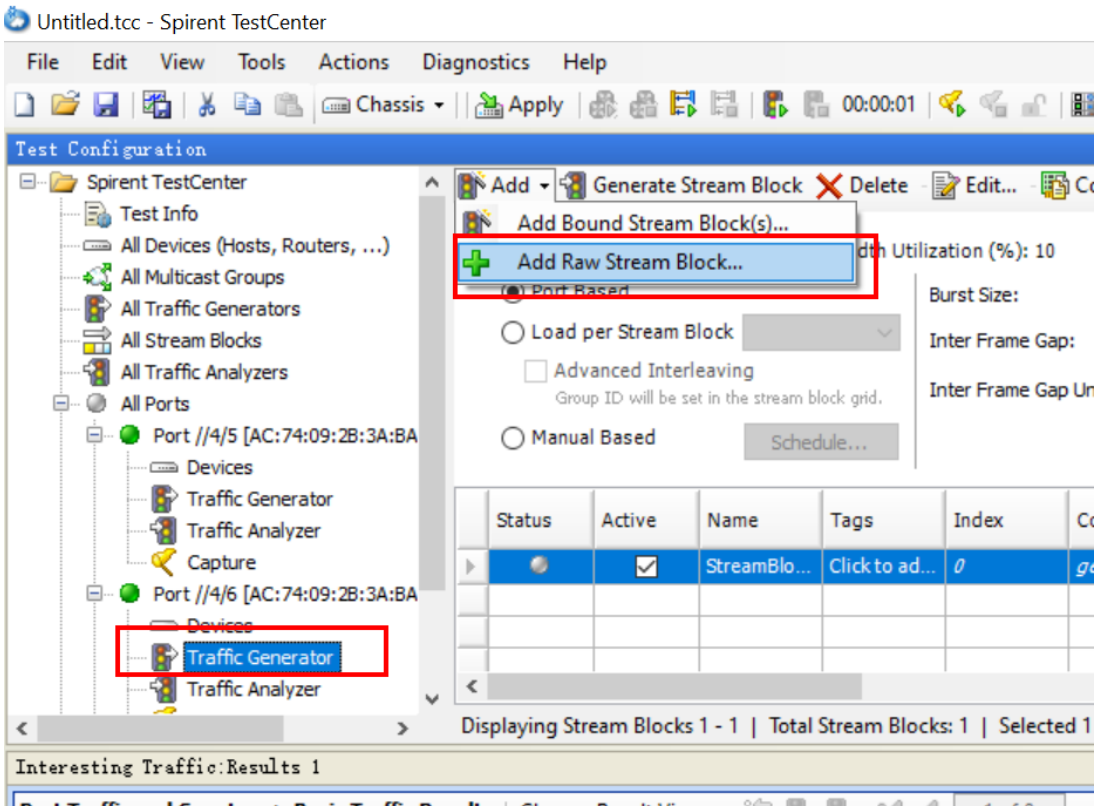

```
[DUT]display mac-address count
100 mac address(es) found.
```

3. On the DUT, set the MAC learning limit to 150 on Port 3.

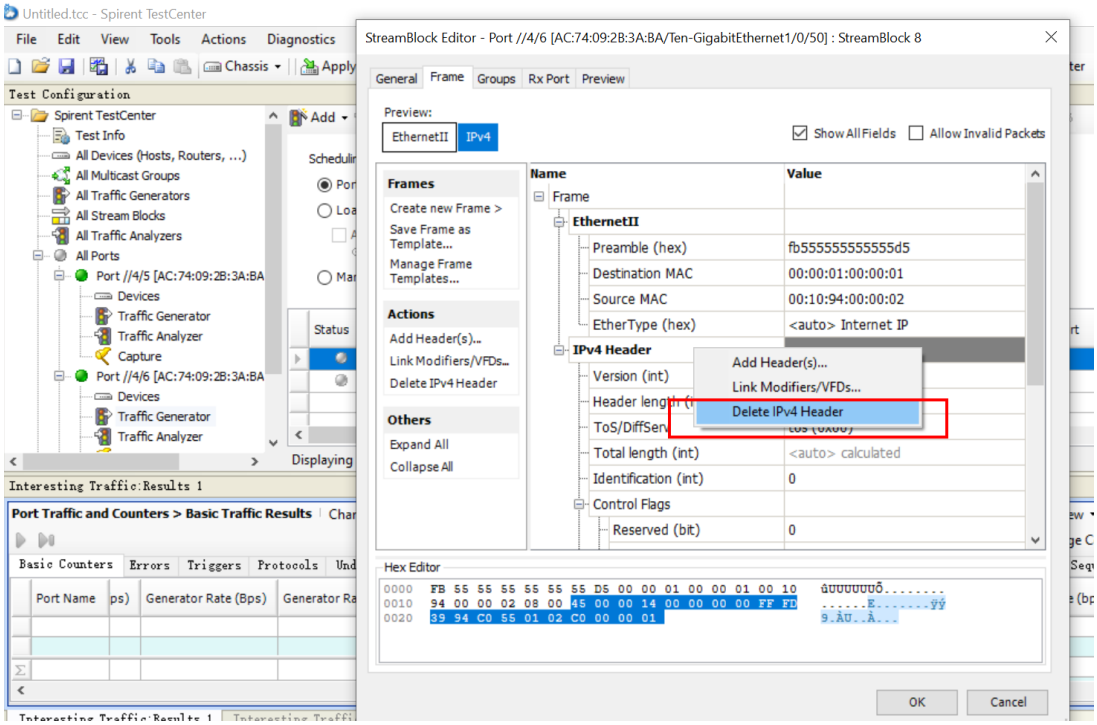
```
[DUT]interface Ten-GigabitEthernet1/0/51
[DUT-Ten-GigabitEthernet1/0/51]mac-address max-mac-count 150
```

4. On the tester, send untagged broadcast packets through Port C. The source MAC addresses of the packets are 1000 consecutive MAC addresses starting at 0-0-1111. Result 2 is expected.

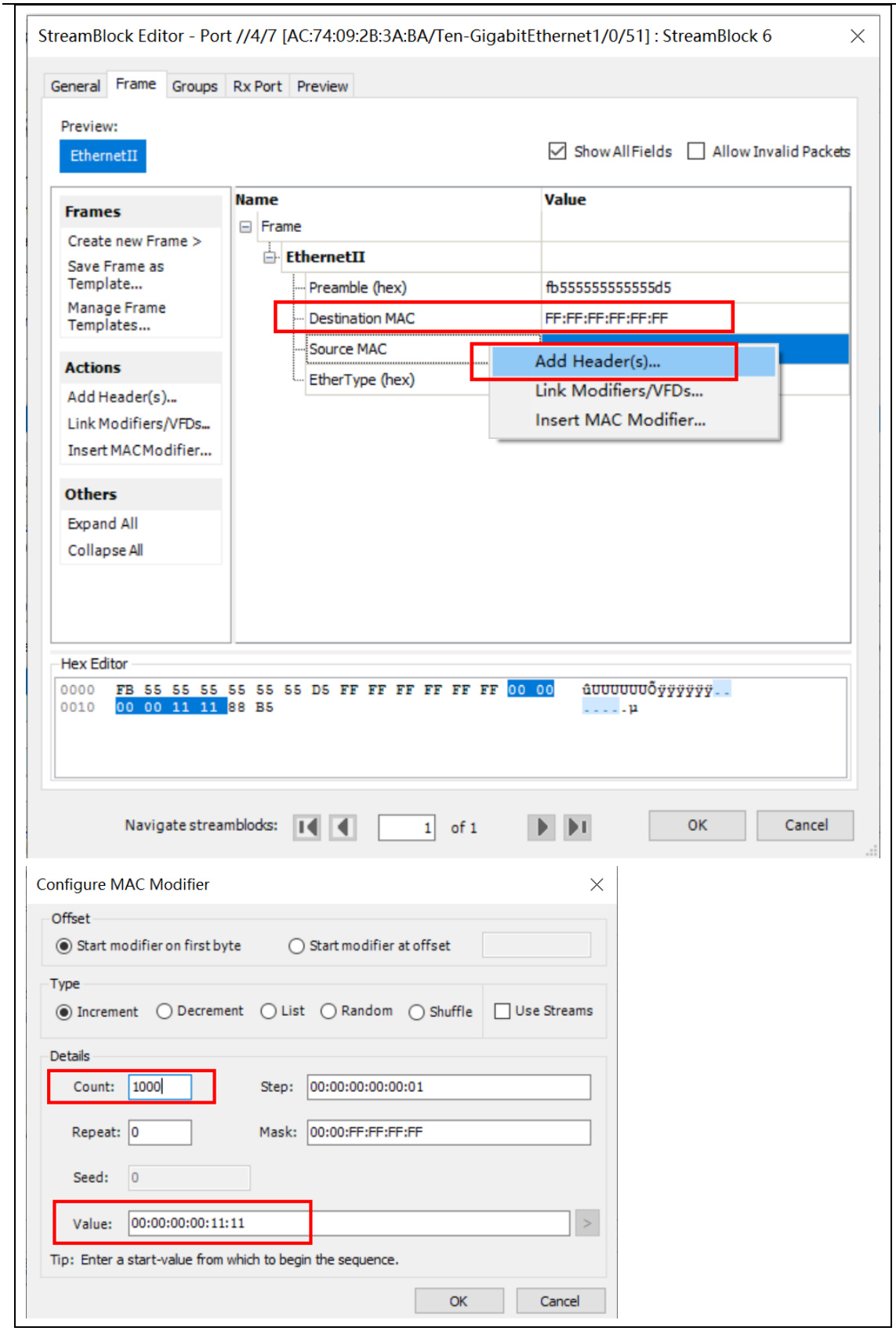
Add raw stream.



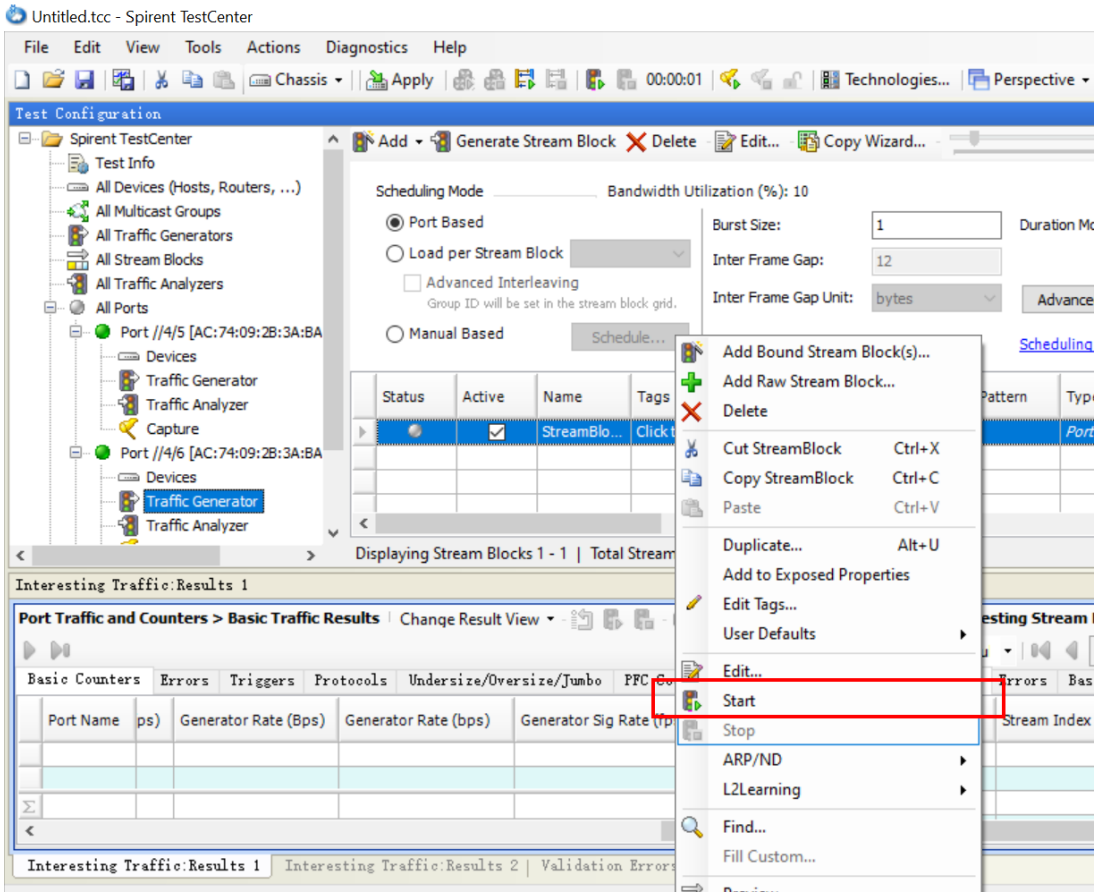
Delete the IPv4 header.

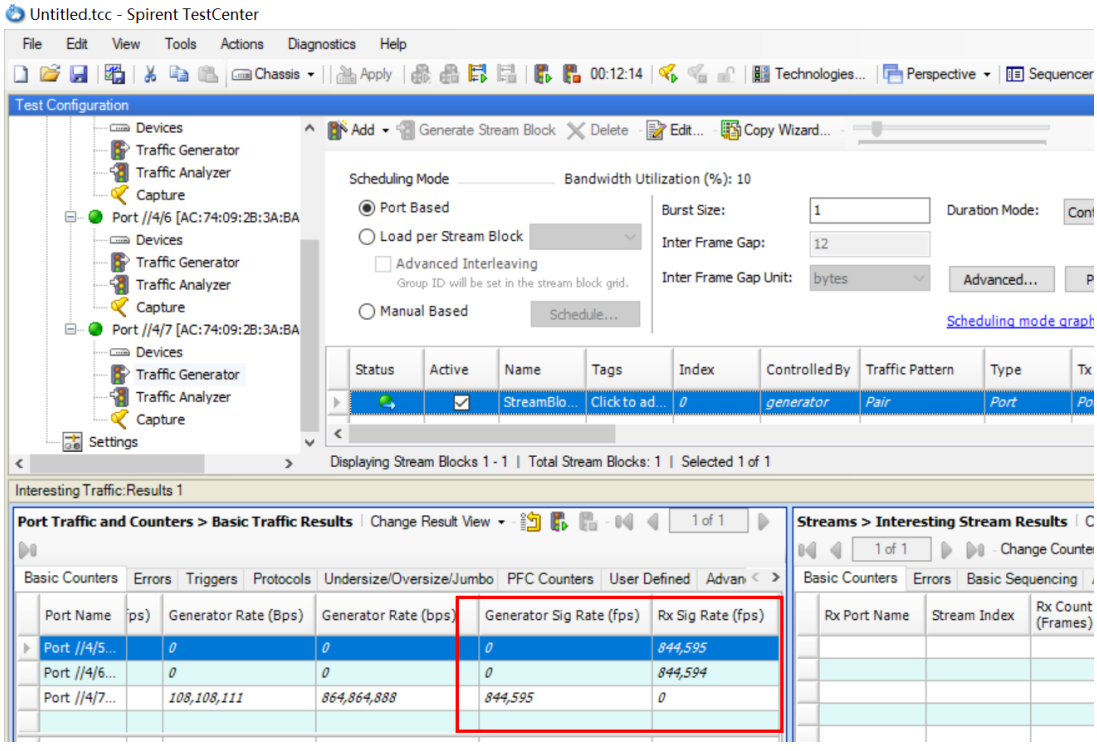


Change the source MAC modifier.


StreamBlock Editor - Port //4/7 [AC:74:09:2B:3A:BA/Ten-GigabitEthernet1/0/51] : StreamBlock 6
General
Frame
Groups
Rx Port
Preview
Preview:
EthernetII
Show All Fields
Allow Invalid Packets
Frames
Create new Frame >
Save Frame as Template...
Manage Frame Templates...
Actions
Add Header(s)...
Link Modifiers/VFDs...
Insert MAC Modifier...
Others
Expand All
Collapse All
Name
Value
Frame
EthernetII
Preamble (hex)
fb555555555555d5
Destination MAC
FF:FF:FF:FF:FF:FF
Source MAC
EtherType (hex)
Add Header(s)...
Link Modifiers/VFDs...
Insert MAC Modifier...
Hex Editor
0000 FB 55 55 55 55 55 55 D5 FF FF FF FF FF FF 00 00
0010 00 00 11 11 88 B5
Navigate streamblocks:
1
of 1
OK
Cancel
Configure MAC Modifier
Offset
Start modifier on first byte
Start modifier at offset
Type
Increment
Decrement
List
Random
Shuffle
Use Streams
Details
Count: 1000
Step: 00:00:00:00:00:01
Repeat: 0
Mask: 00:00:FF:FF:FF:FF
Seed: 0
Value: 00:00:00:00:11:11
Tip: Enter a start-value from which to begin the sequence.
OK
Cancel

Send the traffic.





```
[DUT]display mac-address count
150 mac address(es) found.
```

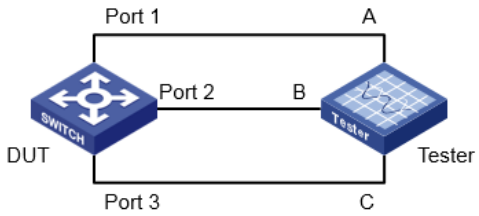
☐ Passed	☐ Failed

2.12 Jumbo frame

Test Item Name: Jumbo Frame

Work Hour: 10 min

Test Topology:



Test Process:

1. Enable jumbo frame forwarding on Port A, Port B, and Port C of Tester.
2. Port A of Tester sends broadcast packets with the length as 9000(9216) bytes continuously. Result 1 is expected.
3. Disable jumbo frame forwarding on Port 1 of DUT1. Result 2 is expected.
4. Enable jumbo frame forwarding on Port 1 of DUT1. Result 1 is expected.

Expect Results:

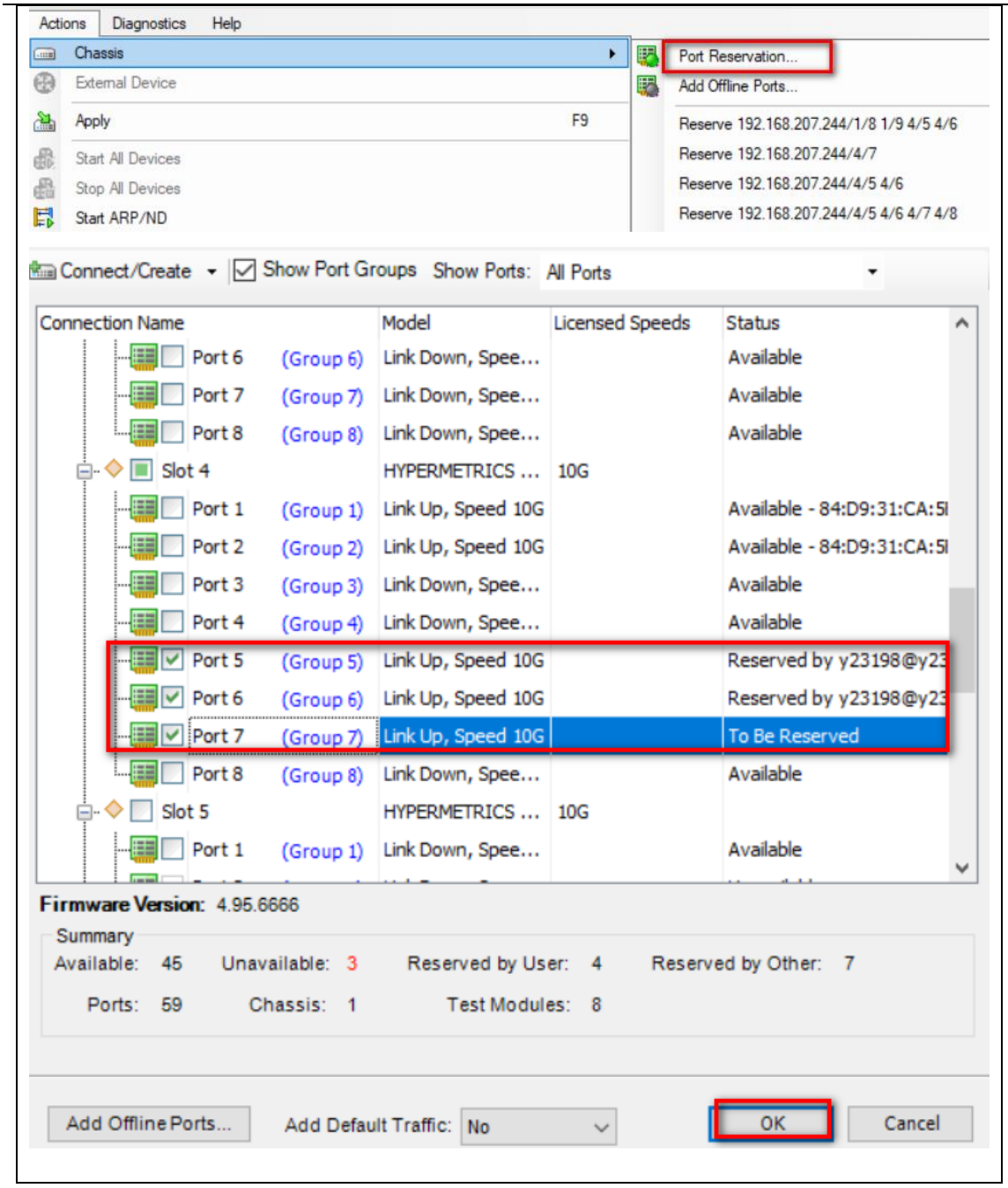
1. Packets sent out Port A of Tester are received on Port B and Port C of Tester.
2. Packets sent out Port A of Tester are not received on Port B and Port C of Tester.

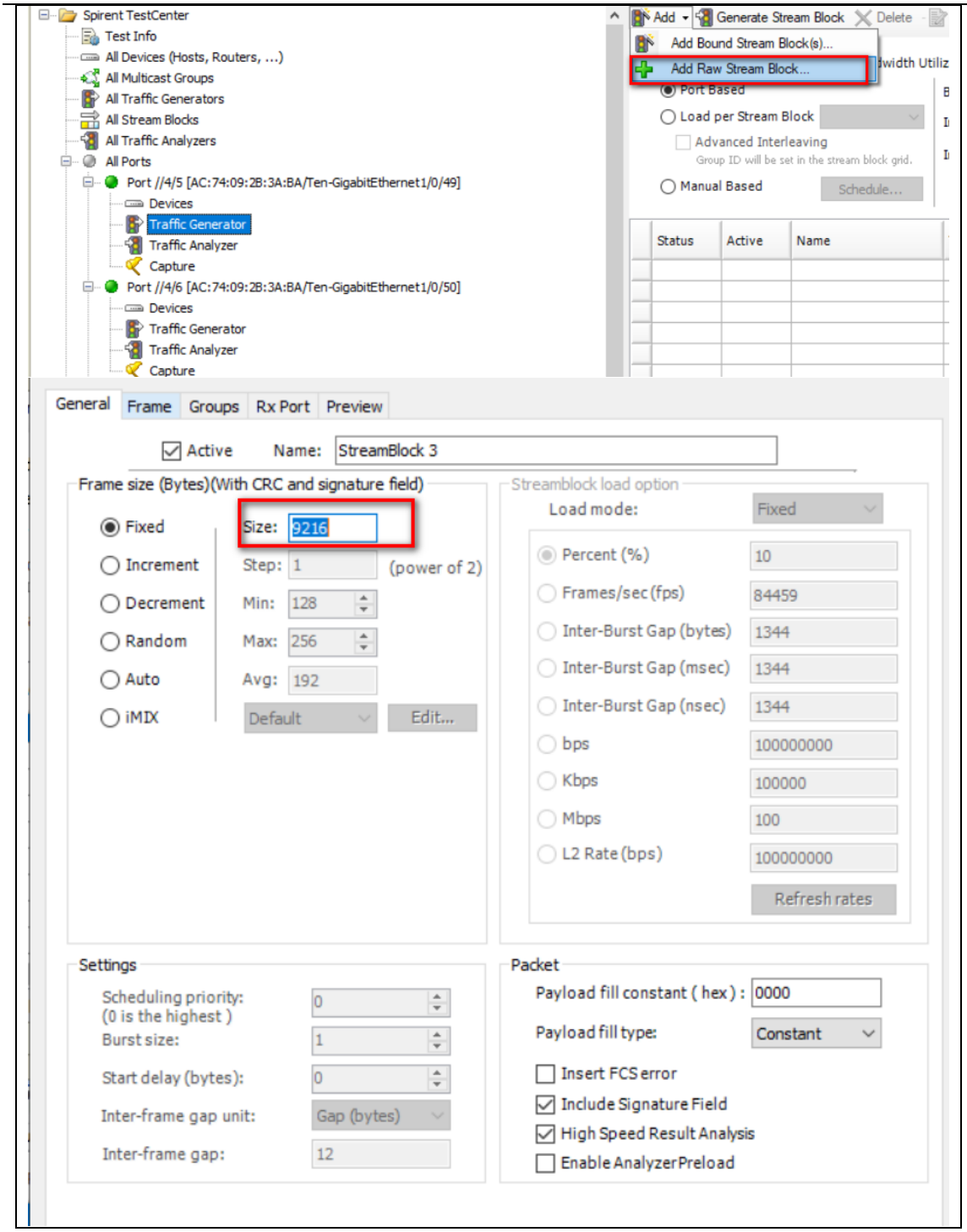
Actual Result：

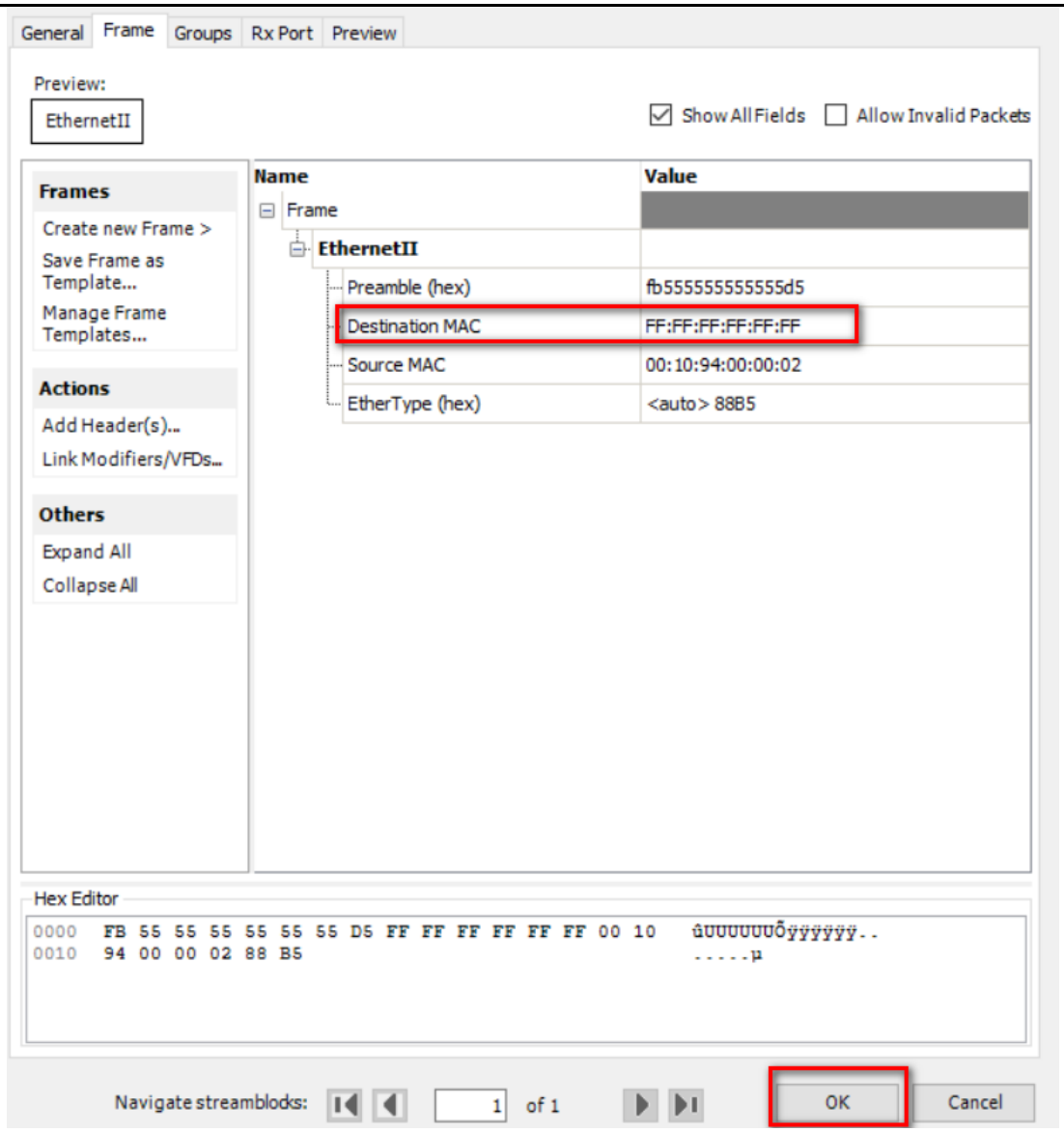
1. Enable jumbo frame forwarding on Port A, Port B, and Port C of Tester

```
[DUT-Ten-GigabitEthernet1/0/49]jumboframe enable
[DUT-Ten-GigabitEthernet1/0/49]interface Ten-GigabitEthernet1/0/50
[DUT-Ten-GigabitEthernet1/0/50]jumboframe enable
[DUT-Ten-GigabitEthernet1/0/50]interface Ten-GigabitEthernet1/0/51
[DUT-Ten-GigabitEthernet1/0/51]jumboframe enable
```

2. Port A of Tester sends broadcast packets with the length as 9000(9216) bytes continuously. Result 1 is expected

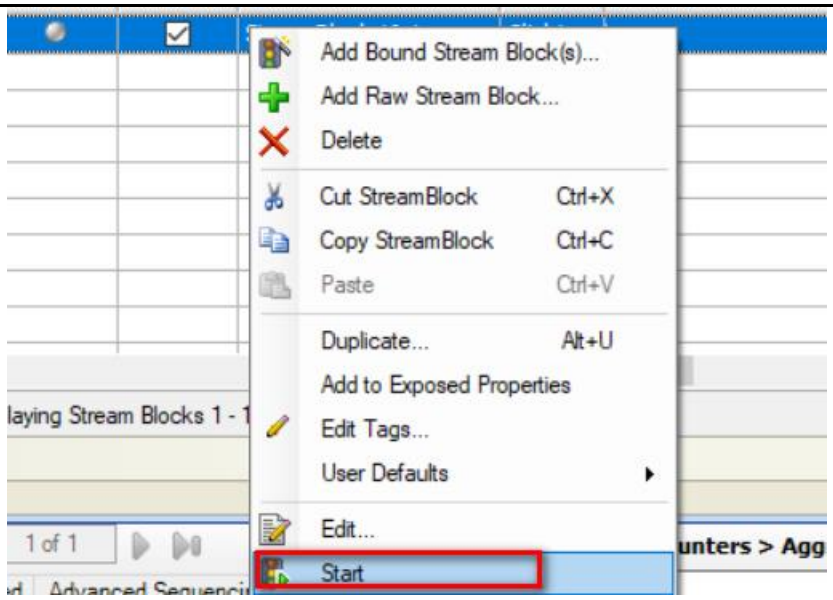






3. Disable jumbo frame forwarding on Port 1 of DUT1. Result 2 is expected

```
[DUT-Ten-GigabitEthernet1/0/49]undo jumboframe enable
```



Port Name	e (fps)	Generator Rate (fps)	Generator Rate (Bps)	Generator Rate (bps)	Generator Sig Rate (fps)	Rx Sig Rate (fps)
Port //4/5...		13,534	124,729,941	997,839,528	13,534	0
Port //4/6...		0	0	0	0	0
Port //4/7...		0	0	0	0	0

4. Enable jumbo frame forwarding on Port 1 of DUT1. Result 1 is expected

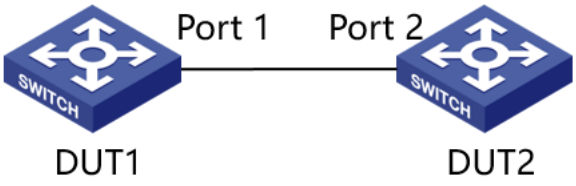
```
[DUT-Ten-GigabitEthernet1/0/49]jumboframe enable
```

Basic Counters | Errors | Triggers | Protocols | Undersize/Oversize/Jumbo | PFC Counters | User Defined | Advanced Sequencing | FEC Counters

Port Name	e (fps)	Generator Rate (fps)	Generator Rate (Bps)	Generator Rate (bps)	Generator Sig Rate (fps)	Rx Sig Rate (fps)
Port //4/5...		13,534	124,729,568	997,836,544	13,534	0
Port //4/6...		0	0	0	0	13,534
Port //4/7...		0	0	0	0	13,534

☐ Passed	☐ Failed

2.13 Ethernet auto negotiation

Test Item Name: Ethernet Auto negotiation
Work Hour: 15 min
Test Topology: 
Test Process:

1. Connect DUT1 with DUT2 on 10GE port, using SFP transceivers. Create VLAN-int on both devices and configure IP addresses. Perform ping between two VLAN-int. Result 1 is expected.
2. Check the status of interface on DUT. Result 2 is expected.

Expect Results:

1. DUT 1/2 can successfully ping each other.
2. The status of interface is 10GE speed

Actual Result:

Configuration on DUT1:

1. Add Port1 to VLAN 10 and assign IP address to VLAN interface 10.

```
[DUT1]vlan 10
[DUT1-vlan10]port Ten-GigabitEthernet 1/0/25
```

```
[DUT1]interface Vlan-interface 10
[DUT1-Vlan-interface10]ip address 30.0.0.1 24
```

Configuration on DUT2:

2. Add Port2 to VLAN 10 and assign IP address to VLAN interface 10.

```
[DUT2]vlan 10
[DUT2-vlan10]port Ten-GigabitEthernet 1/0/52
```

```
[DUT2]interface Vlan-interface 10
[DUT2-Vlan-interface10]ip address 30.0.0.2 24
```

3. Perform ping between two VLAN-int. Result 1 is expected.

```
[DUT1]ping 30.0.0.2
Ping 30.0.0.2 (30.0.0.2): 56 data bytes, press CTRL+C to break
56 bytes from 30.0.0.2: icmp_seq=0 ttl=255 time=1.922 ms
56 bytes from 30.0.0.2: icmp_seq=1 ttl=255 time=1.744 ms
56 bytes from 30.0.0.2: icmp_seq=2 ttl=255 time=1.771 ms
56 bytes from 30.0.0.2: icmp_seq=3 ttl=255 time=43.703 ms
56 bytes from 30.0.0.2: icmp_seq=4 ttl=255 time=1.787 ms

--- Ping statistics for 30.0.0.2 ---
5 packet(s) transmitted, 5 packet(s) received, 0.0% packet loss
round-trip min/avg/max/std-dev = 1.744/10.185/43.703/16.759 ms
```

```
[DUT2-Vlan-interface10]ping 30.0.0.1
Ping 30.0.0.1 (30.0.0.1): 56 data bytes, press CTRL+C to break
56 bytes from 30.0.0.1: icmp_seq=0 ttl=255 time=4.806 ms
56 bytes from 30.0.0.1: icmp_seq=1 ttl=255 time=9.865 ms
56 bytes from 30.0.0.1: icmp_seq=2 ttl=255 time=1.655 ms
56 bytes from 30.0.0.1: icmp_seq=3 ttl=255 time=1.680 ms
56 bytes from 30.0.0.1: icmp_seq=4 ttl=255 time=1.519 ms

--- Ping statistics for 30.0.0.1 ---
5 packet(s) transmitted, 5 packet(s) received, 0.0% packet loss
round-trip min/avg/max/std-dev = 1.519/3.905/9.865/3.226 ms
```

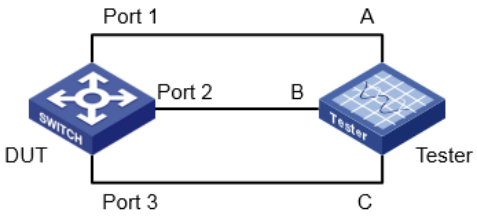
4. Check the status of interface on DUT. Result 2 is expected.

```
[DUT1]display interface Ten-GigabitEthernet 1/0/25
Ten-GigabitEthernet1/0/25
Current state: UP
Line protocol state: UP
IP packet frame type: Ethernet II, hardware address: 7485-c4f6-214a
Description: Ten-GigabitEthernet1/0/25 Interface
Bandwidth: 10000000 kbps
```

```
[DUT2]display interface Ten-GigabitEthernet 1/0/52
Ten-GigabitEthernet1/0/52
Current state: UP
Line protocol state: UP
IP packet frame type: Ethernet II, hardware address: ac74-092b-3b16
Description: Ten-GigabitEthernet1/0/52 Interface
Bandwidth: 10000000 kbps
```

☐ Passed	☐ Failed

2.14 QinQ

Test Item Name: QinQ
Work Hour: 30 min
Test Topology: 
Test Process:

1. On the DUT, create VLAN 2, and assign Port 1 to VLAN 2 as an access port. Configure Port 2 as a hybrid port, and assign Port 2 to VLAN 2 as a tagged member.
2. Enable QinQ on Port 1 of the DUT.
3. Send a broadcast packet tagged with VLAN 100 from Port A of the tester to the DUT. Result 1 is expected.
4. Configure Port 1 of the DUT as a trunk port, and assign it to VLAN 2 and other VLANs. The PVID of Port 1 is 2. Configure Port 2 of the DUT as a hybrid port, and assign it to VLAN 2 as a tagged member.
5. Enable QinQ on Port 1 of the DUT.
6. Send a broadcast packet tagged with VLAN 100 from Port A of the tester to the DUT. Result 1 is expected.

Expect Results:

1. Port B of the tester receives a double-tagged packet from Port 2 of the DUT. The SVLAN and CVLAN of packet is 2 and 100, respectively. The TPID value is 8100 in both the SVLAN tag and the CVLAN tag.

Actual Result：

1. On the DUT, create VLAN 2, and assign Port 1 to VLAN 2 as an access port. Configure Port 2 as a hybrid port, and assign Port 2 to VLAN 2 as a tagged member.

[5560x-ei-1-Ten-GigabitEthernet1/0/25]port access vlan 2

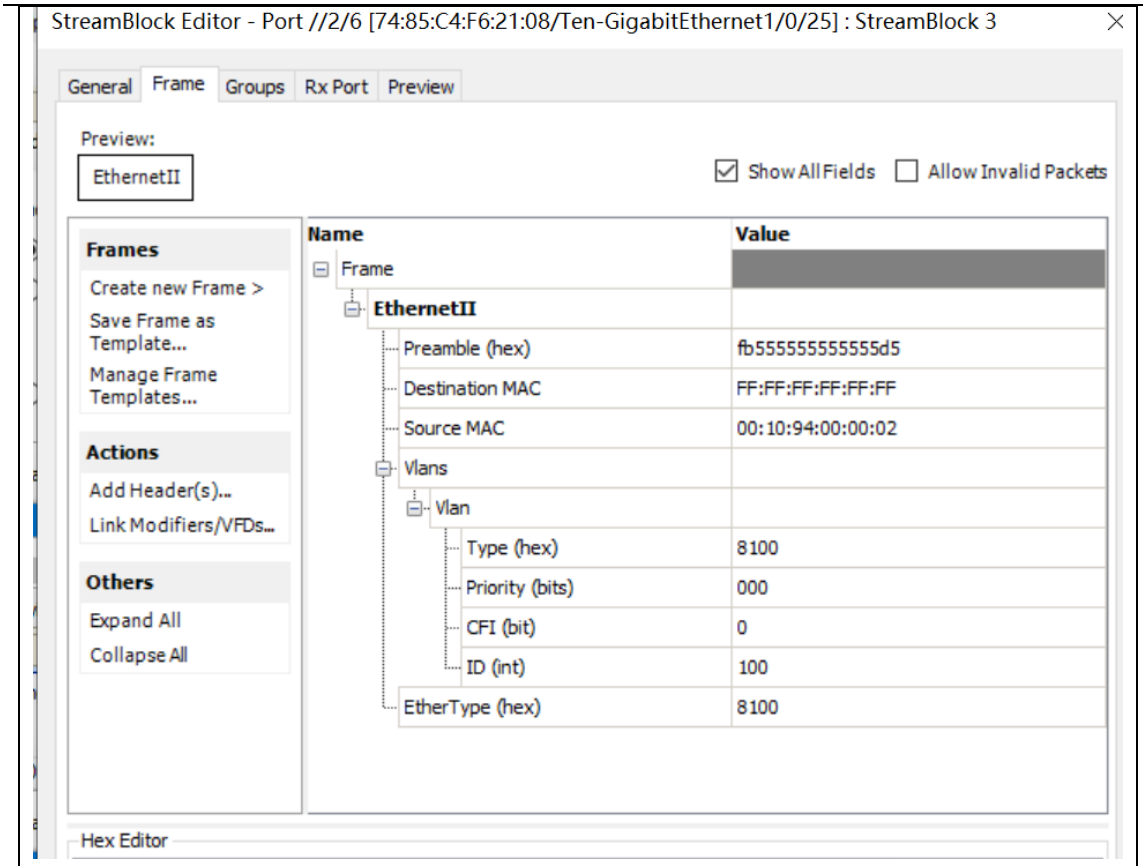
[5560x-ei-1-Ten-GigabitEthernet1/0/26]port link-type hybrid

[5560x-ei-1-Ten-GigabitEthernet1/0/26]port hybrid vlan 2 tagged

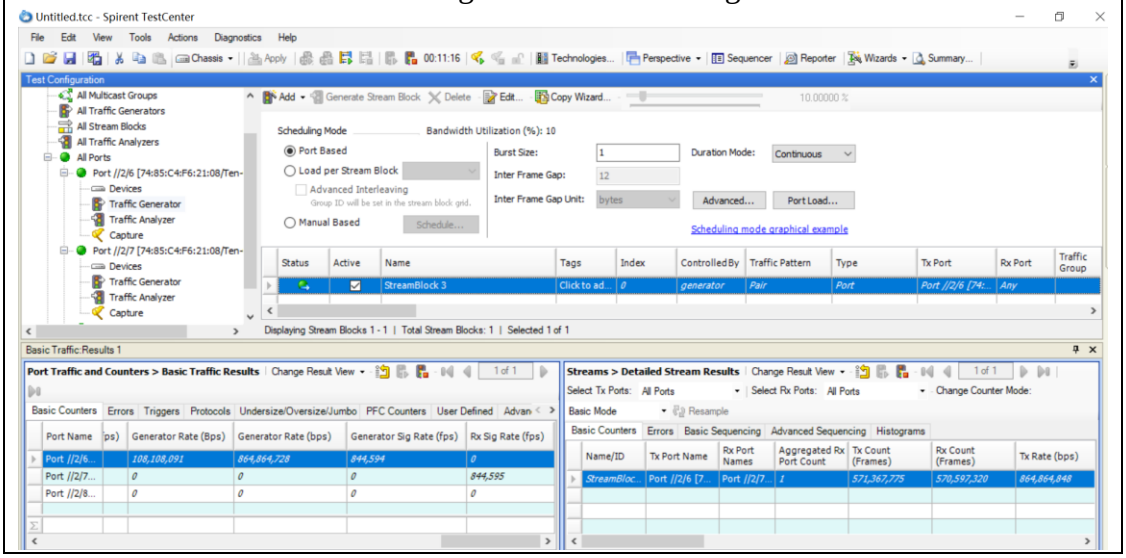
2. Enable QinQ on Port 1 of the DUT.

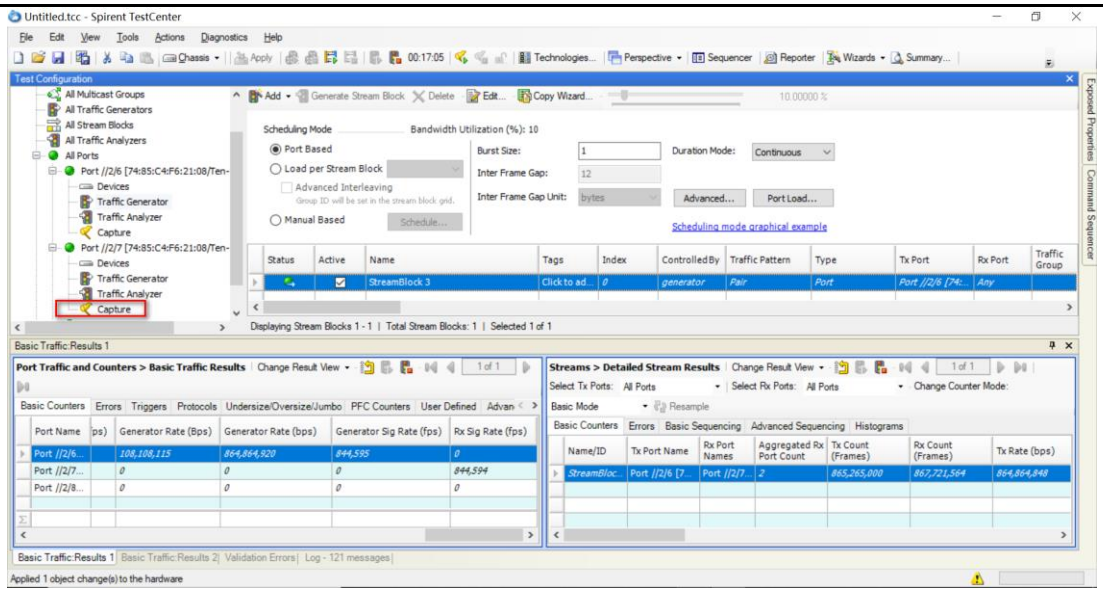
[5560x-ei-1-Ten-GigabitEthernet1/0/25]qinq enable

3. Send a broadcast packet tagged with VLAN 100 from Port A of the tester to the DUT. Result 1 is expected.

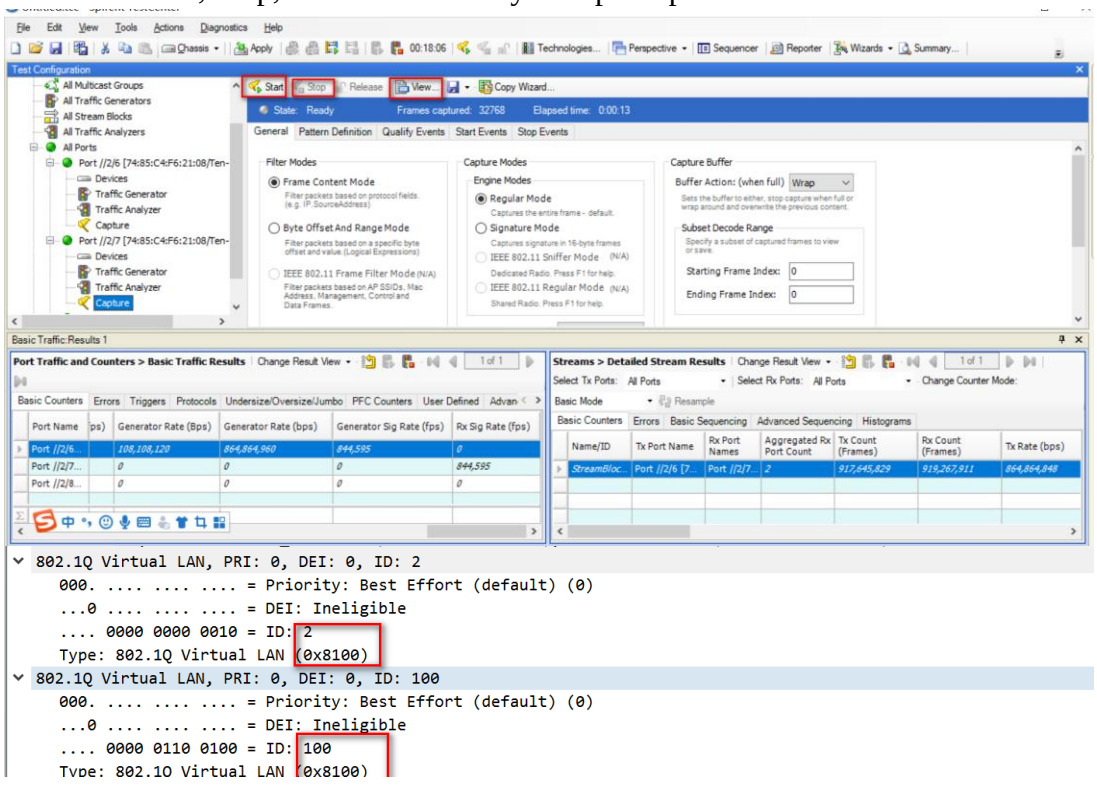


4. Port B of the tester receives a double-tagged packet from Port 2 of the DUT. The SVLAN and CVLAN of packet is 2 and 100, respectively. The TPID value is 8100 in both the SVLAN tag and the CVLAN tag.





Click Start, Stop, View successively to capture packets on Port B of Tester.



```
802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 2
    000. .... .... .... = Priority: Best Effort (default) (0)
    ...0 .... .... .... = DEI: Ineligible
    .... 0000 0000 0010 = ID: 2
    Type: 802.1Q Virtual LAN (0x8100)
802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 100
    000. .... .... .... = Priority: Best Effort (default) (0)
    ...0 .... .... .... = DEI: Ineligible
    .... 0000 0110 0100 = ID: 100
    Type: 802.1Q Virtual LAN (0x8100)
```

5. Configure Port 1 of the DUT as a trunk port, and assign it to VLAN 2 and other VLANs. The PVID of Port 1 is 2. Configure Port 2 of the DUT as a hybrid port, and assign it to VLAN 2 as a tagged member.

#

interface Ten-GigabitEthernet1/0/26

port link-mode bridge

port link-type hybrid

port hybrid vlan 2 tagged

port hybrid vlan 1 untagged

#

interface Ten-GigabitEthernet1/0/25

port link-mode bridge

port link-type trunk

port trunk permit vlan all

port trunk pvid vlan 2

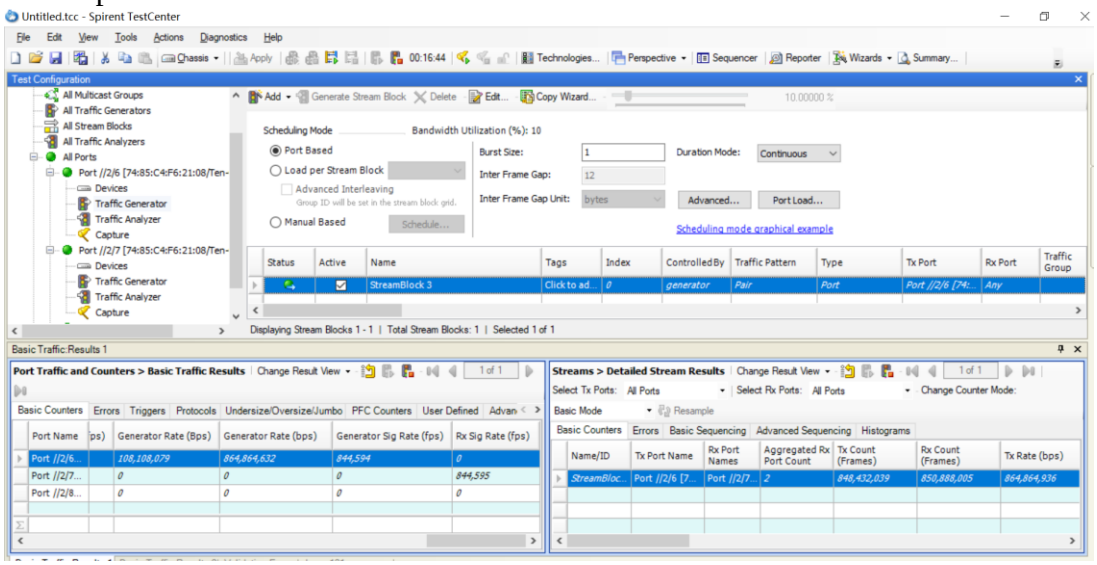
qinq enable

#

6. Enable QinQ on Port 1 of the DUT.

qinq enable

7. Capture on Port B of tester

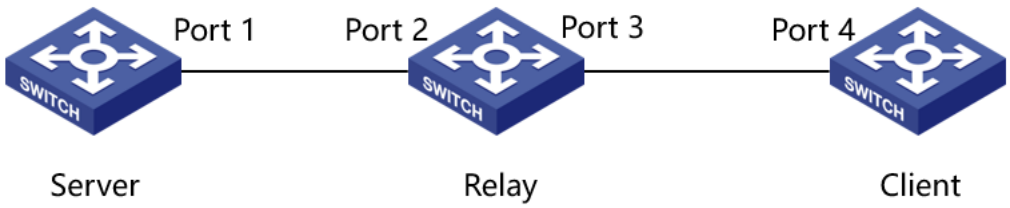



```
Frame 1: 132 bytes on wire (1056 bits), 132 bytes captured (1056 bits) on interface \\.\pipe\view_capture_192-168-207-244_2_7_01292021_150813, id
Ethernet II, Src: Performa_00:00:02 (00:10:94:00:00:02), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 2
    000. .... .... .... = Priority: Best Effort (default) (0)
    ...0 .... .... .... = DEI: Ineligible
    .... 0000 0000 0010 = ID: 2
    Type: 802.1Q Virtual LAN (0x8100)
802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 100
    000. .... .... .... = Priority: Best Effort (default) (0)
    ...0 .... .... .... = DEI: Ineligible
    .... 0000 0110 0100 = ID: 100
    Type: 802.1Q Virtual LAN (0x8100)
```

☐ Passed	☐ Failed

3 Layer 3 protocol

3.1 DHCP

Test Item Name: DHCP
Work Hour：30 min
Test Topology: 
Test Process: 1. Configure the DHCP server and relay on DUT 2. Configure the DHCP relay agent to support Option 82. 3. Configure the strategy for handling DHCP requests containing Option 82. 4. Configure the padding mode for the Circuit ID sub-option and the Remote ID sub-option of Option 82. 5. Configure Port 4 to request an IP address from the DHCP server. Result 1 is expected. 6. Use the Wireshark to capture packets on the server. Configure DUT 2 to request an IP address from the DHCP server again. Result 2 is expected.
Expect Results: 1. Port 4 can get IP address from DHCP server. 2. The captured DHCP discover packet contains the Circuit ID sub-option and the Remote ID sub-option of Option 82
Actual Result： Configuration on DHCP Server： 1. Add Port4 to VLAN and assign IP address to VLAN interface.

```
[DHCP Server]vlan 20
[DHCP Server-vlan20]port GigabitEthernet 1/0/1
[DHCP Server-vlan20]interface Vlan-interface 20
[DHCP Server-Vlan-interface20]ip address 20.0.0.1 255.255.255.0
```

2. Enable DHCP

```
[DHCP Server]dhcp enable
```

3. Exclude the IP addresses of the gateway from dynamic assignment.

```
[DHCP Server]dhcp server forbidden-ip 10.0.0.1
```

4. Configure parameters in DHCP address pool 0, including the subnet for address assignment and gateway address.

```
[DHCP Server]dhcp server ip-pool 1
[DHCP Server-dhcp-pool-1]network 10.0.0.0 mask 255.255.255.0
[DHCP Server-dhcp-pool-1]gateway-list 10.0.0.1
```

5. Apply DHCP address pool 1 to VLAN-interface 20 on the DUT.

```
[DHCP Server]int vlan 20
[DHCP Server-Vlan-interface20]dhcp server apply ip-pool 1
```

Configuration on DHCP Relay：

6. Enable DHCP on DUT.

```
[DHCP Relay]dhcp enable
```

7. Create a VLAN interface that is connected to the DHCP server.

```
[DHCP Relay]vlan 20
[DHCP Relay-vlan20]port GigabitEthernet 1/0/1
[DHCP Relay-vlan20]interface Vlan-interface 20
[DHCP Relay-Vlan-interface20]ip address 20.0.0.2 24
```

8. Create VLAN 100 and enable the DHCP relay agent on VLAN-interface 100

```
[DHCP Relay]vlan 100
[DHCP Relay-vlan100]port GigabitEthernet 1/0/2
[DHCP Relay-vlan100]interface Vlan-interface 100
[DHCP Relay-Vlan-interface100]ip address 10.0.0.1 24
[DHCP Relay-Vlan-interface100]dhcp select relay
```

9. Specify the DHCP server address on VLAN-interface 100.

```
[DHCP Relay]interface Vlan-interface 100
[DHCP Relay-Vlan-interface100]dhcp relay server-address 20.0.0.1
```

10. Configure the DHCP relay agent to support Option 82.

```
[DHCP Relay-Vlan-interface100]dhcp relay information enable
```

11. Configure the strategy for handling DHCP requests containing Option 82.

```
[DHCP Relay-Vlan-interface100]dhcp relay information strategy replace
```

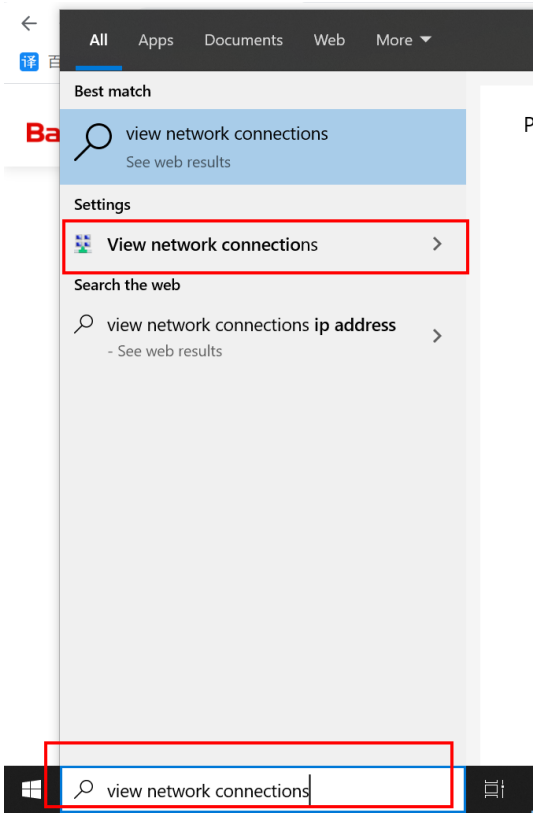
12. Configure the padding mode and padding format of Option 82.

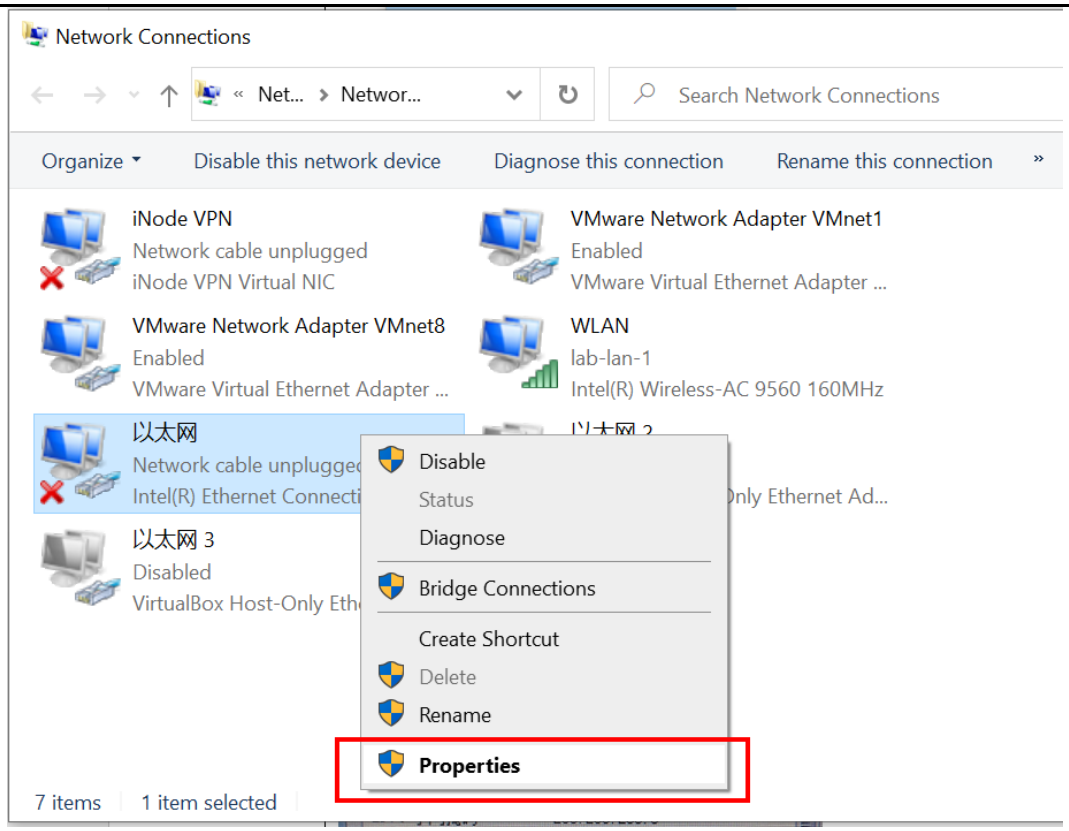
```
[DHCP Relay-Vlan-interface100]dhcp relay information remote-id string normal
[DHCP Relay-Vlan-interface100]dhcp relay information circuit-id normal
```

13. Configure the DHCP client to request an IP address from the DHCP server.

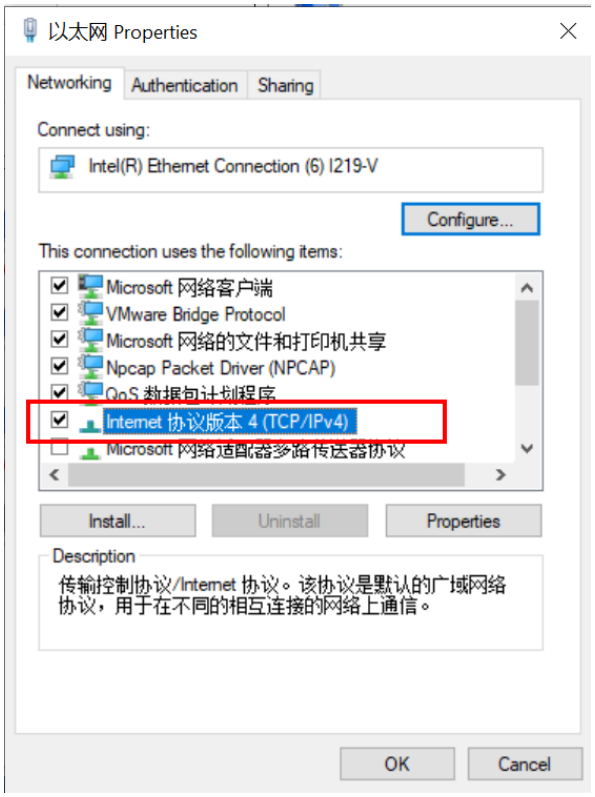
    Result 1 is expected.

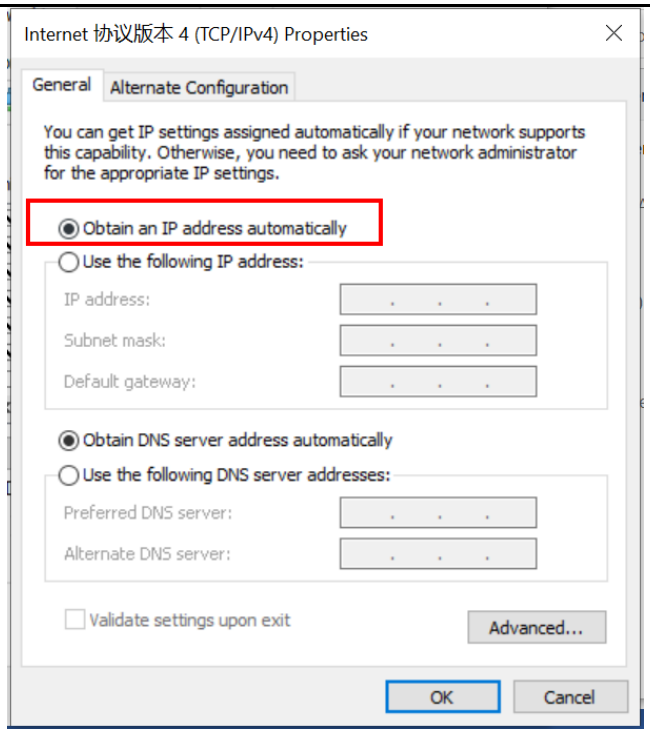
Select computer network card



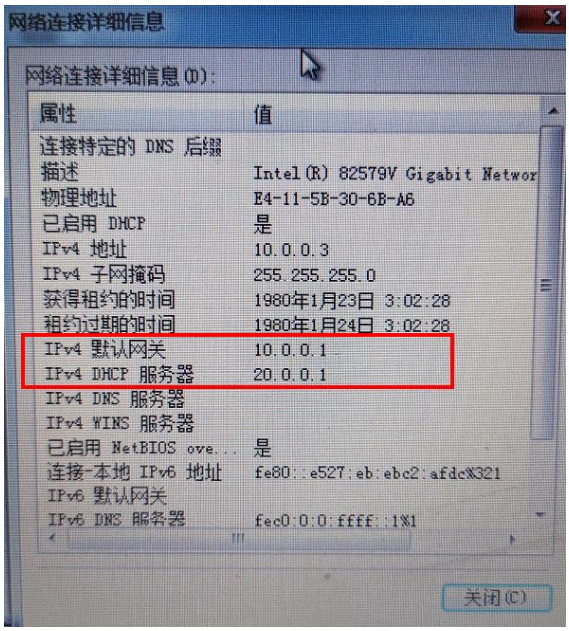


Set the network card to obtain IP address automatically



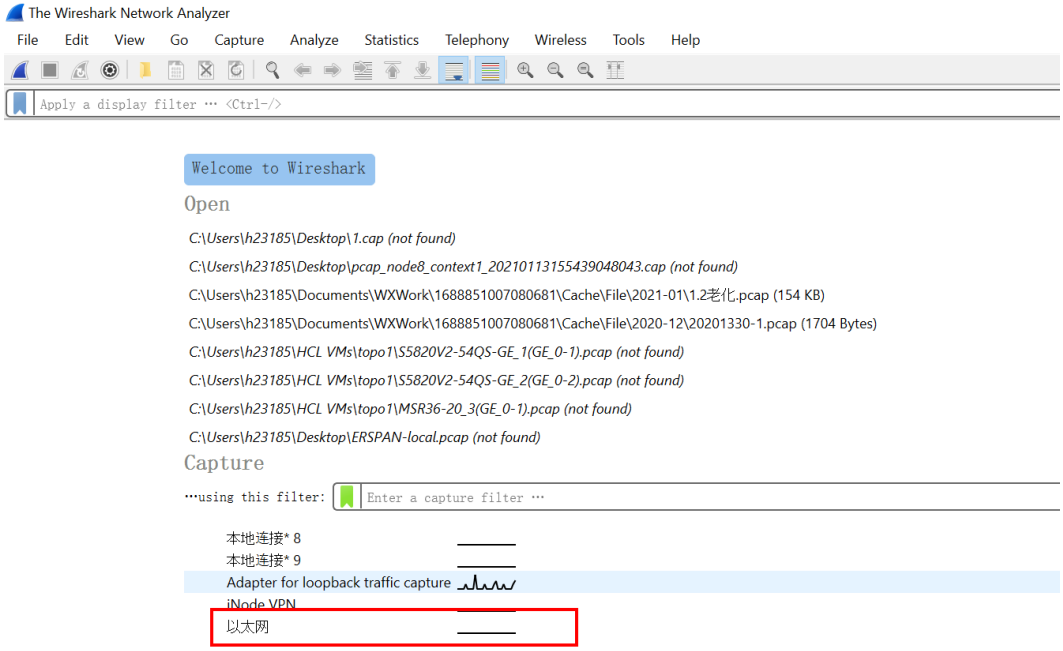


The client can get IP address from DHCP server.

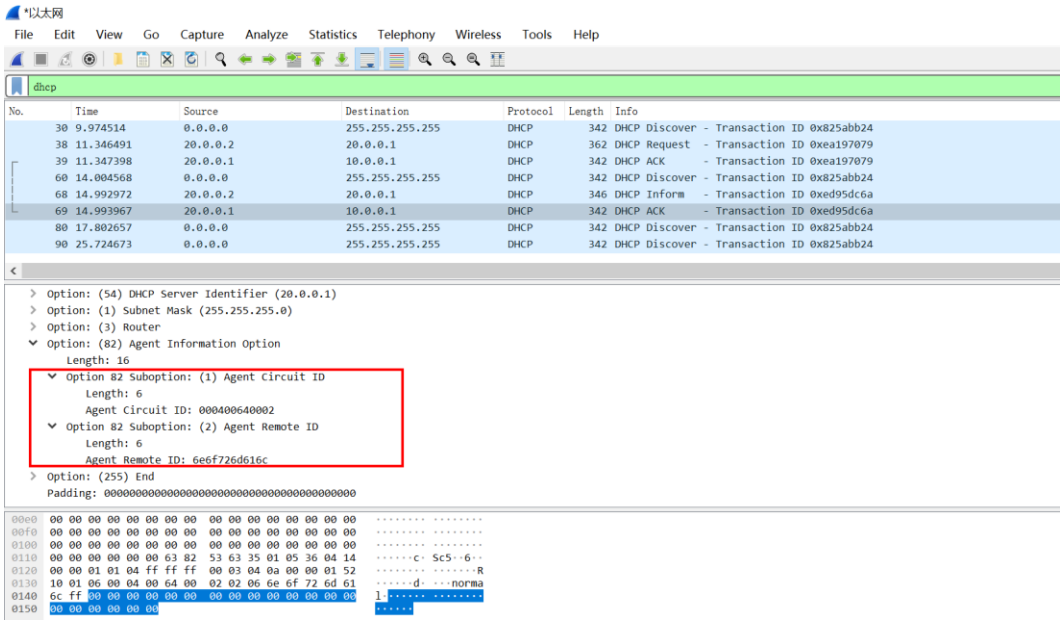


14. Use the Wireshark to capture packets on the server. Configure client to request an IP address from the DHCP server again. Result 2 is expected.

Select the corresponding network card on Wireshark.



The captured DHCP discover packet contains the Circuit ID sub-option and the Remote ID sub-option of Option 82.



☐ Passed	☐ Failed

3.2 OSPF

Test Item Name: OSPF

Work Hour：20 min

Test Topology:

Test Process:

1. Configure IP addresses for Port1 and Port2
2. Configure IP addresses for Loopback interfaces on DUT1 and DUT2
3. Configure OSPF on DUT1 and DUT2 with expect Result 1
4. Check the routing-table on DUT1 and DUT2 with expect Result 2
5. Perform ping between the two loopback interfaces.

Expect Results:

1. DUT1 and DUT2 can build OSPF neighbors
2. The loopback routing can be seen in the routing-table, and its type is OSPF
3. DUT1 and DUT2 can successfully ping each other.

Actual Result：

1. Configure IP addresses for Port1 and Port2

DUT1：

int Ten-GigabitEthernet 1/0/25-----port 1

ip address 10.2.1.1 24

DUT2：

int Ten-GigabitEthernet 1/0/2-----port 2

ip address 10.2.1.2 24

2. Configure IP addresses for Loopback interfaces on DUT1 and DUT2

DUT1：

int loopback 0

ip address 1.1.1.1 32

DUT2：

int loopback 0

ip address 2.2.2.2 32

3. Configure OSPF on DUT1 and DUT2

```
[5560x-ei-1-ospf-1]d%Jan  4 02:33:53:399 2013 5560x-ei-1 OSPF/5/OSPF_NBR_CHG: O
SPF 1 Neighbor 10.2.1.2(Ten-GigabitEthernet1/0/25) changed from LOADING to FULL
.
dis ospf peer

         OSPF Process 1 with Router ID 10.2.1.1
               Neighbor Brief Information

 Area: 0.0.0.0
 Router ID       Address         Pri Dead-Time  State             Interface
 10.2.1.2        10.2.1.2        1   38         Full/DR           XGE1/0/25
[5560x-ei-1-ospf-1]
```

4. Check the routing-table on DUT1 and DUT2.

```
[5560x-ei-1-ospf-1-area-0.0.0.0]dis ip routing-table

Destinations : 21       Routes : 21

Destination/Mask    Proto   Pre Cost        NextHop         Interface
0.0.0.0/32          Direct  0   0           127.0.0.1       InLoop0
1.1.1.0/24          Direct  0   0           1.1.1.1         Loop0
1.1.1.0/32          Direct  0   0           1.1.1.1         Loop0
1.1.1.1/32          Direct  0   0           127.0.0.1       InLoop0
1.1.1.255/32        Direct  0   0           1.1.1.1         Loop0
2.2.2.2/32          O_INTRA 10  1           10.2.1.2        XGE1/0/25
10.2.1.0/24         Direct  0   0           10.2.1.1        XGE1/0/25
10.2.1.0/32         Direct  0   0           10.2.1.1        XGE1/0/25
10.2.1.1/32         Direct  0   0           127.0.0.1       InLoop0
10.2.1.255/32       Direct  0   0           10.2.1.1        XGE1/0/25
127.0.0.0/8         Direct  0   0           127.0.0.1       InLoop0
127.0.0.0/32        Direct  0   0           127.0.0.1       InLoop0
127.0.0.1/32        Direct  0   0           127.0.0.1       InLoop0
127.255.255.255/32  Direct  0   0           127.0.0.1       InLoop0
192.168.206.0/23    Direct  0   0           192.168.207.140 MGE0/0/0
192.168.206.0/32    Direct  0   0           192.168.207.140 MGE0/0/0
192.168.207.140/32  Direct  0   0           127.0.0.1       InLoop0
```

ping each other

```
<5560x-ei-1>ping -a 1.1.1.1 2.2.2.2
Ping 2.2.2.2 (2.2.2.2) from 1.1.1.1: 56 data bytes, press CTRL+C to break
56 bytes from 2.2.2.2: icmp_seq=0 ttl=255 time=2.575 ms
56 bytes from 2.2.2.2: icmp_seq=1 ttl=255 time=1.778 ms
56 bytes from 2.2.2.2: icmp_seq=2 ttl=255 time=1.717 ms
56 bytes from 2.2.2.2: icmp_seq=3 ttl=255 time=1.746 ms
```

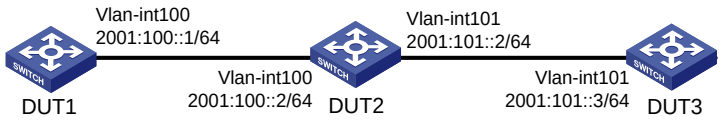
☐ Passed	☐ Failed

3.3 OSPFv3 authentication

Test Item Name: OSPFv3 authentication

Work Hour：20 min

Test Topology:



Test Process:

1. Enable OSPFv3 routing protocols on devices DUT1, DUT2, and DUT3 respectively; OSPFv3 configuration on device DUT1 is as follows, and OSPFv3 configuration on devices DUT2 and DUT3 is similar：
2. Configure the encryption rule set, configure the authentication algorithm as HMAC-SHA-256, and configure the verification password and effective time
3. Enable keychain authentication on the Layer 3 interface
4. Check the status of ospfv3 neighbors on display DUT1 / DUT2 / DUT3 via display ospfv3 peer, the result 1 is expected.
5. The device DUT1 pings the IPv6 address of the VLAN101 virtual interface of device DUT3, or the device DUT3 pings the IPv6 address of the VLAN100 virtual interface of device DUT1, the result 2 is expected.

Expect Results:

1. OSPFv3 neighbor established correctly
2. Able to ping.

Actual Result：

1. Configurations on DUTs,

DUT1/2/3:

```
#
ospfv3 1
 router-id 1.1.1.1/2.2.2.2/3.3.3.3
#
```

Enable OSPFv3 on each VLAN-interface respectively

```
#
interface Vlan-interface100
 ospfv3 1 area 0.0.0.0
#
```

#
keychain test mode absolute
key 1
key-string plain 123456
authentication-algorithm hmac-sha-256
send-lifetime utc 11:11:11 2021/01/01 to 11:11:11 2022/01/01
accept-lifetime utc 11:11:11 2021/01/01 to 11:11:11 2022/01/01
#
Note: The system time should be among 11:11:11 2021/01/01 to 11:11:11 2022/01/01, then the keychain will take effect.

2. Enable keychain authentication on the Layer 3 interface
   Enter the Layer 3 interface
   Ospfv3 authentication-mode keychain test
3. Check the status of ospfv3 neighbors on display Dos1 / DUT2 / DUT3 via display ospfv3 peer, the result 1 is expected.
   Put command **dis ospf peer** on all devices to check the result.
4. OSPFv3 neighbor established correctly

```
dis ospfv3 peer

              OSPFv3 Process 1 with Router ID 2.2.2.2

 Area: 0.0.0.0
--------------------------------------------------------------------------
 Router ID       Pri State             Dead-Time InstID Interface
 3.3.3.3         1   Full/DROther      00:00:38  0      XGE1/0/19
 1.1.1.1         1   Full/DR           00:00:37  0      XGE1/0/21
```

5. Able to ping.

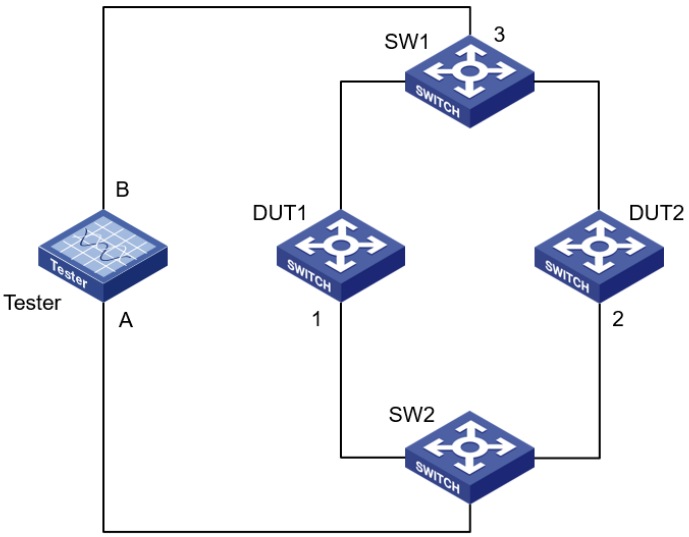
```
ping ipv6 2001:101::3
Ping6(56 data bytes) 2001:100::1 --> 2001:101::3, press CTRL+C to break
56 bytes from 2001:101::3, icmp_seq=0 hlim=63 time=4.658 ms
56 bytes from 2001:101::3, icmp_seq=1 hlim=63 time=2.131 ms
56 bytes from 2001:101::3, icmp_seq=2 hlim=63 time=2.063 ms
56 bytes from 2001:101::3, icmp_seq=3 hlim=63 time=1.916 ms
56 bytes from 2001:101::3, icmp_seq=4 hlim=63 time=2.117 ms

--- Ping6 statistics for 2001:101::3 ---
5 packet(s) transmitted, 5 packet(s) received, 0.0% packet loss
```

☐ Passed	☐ Failed

3.4 BFD for VRRP

Test Item Name: BFD for VRRP
Work Hour：45 min

Test Topology:

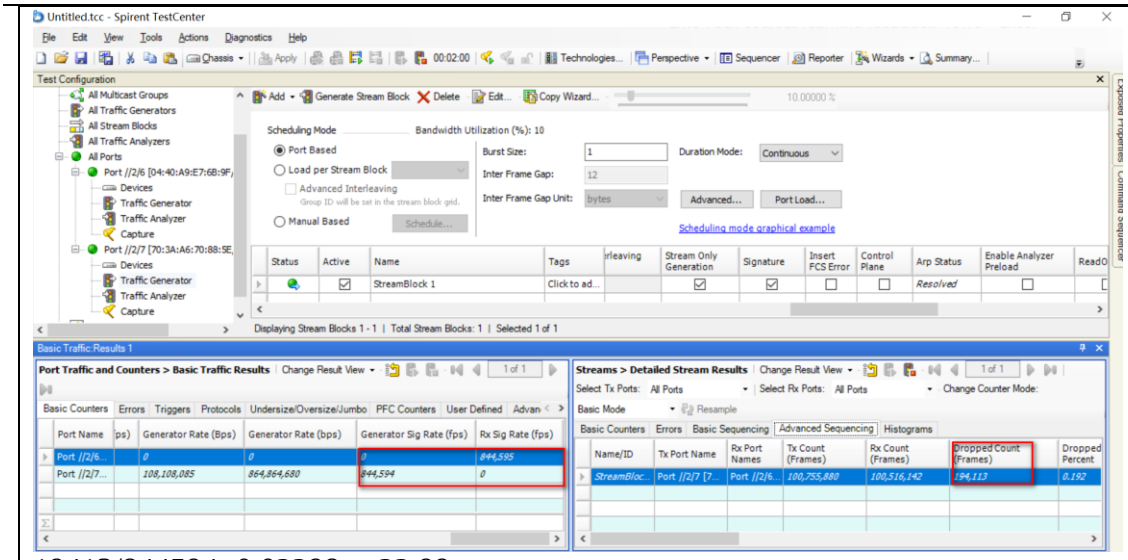


Test Process:

1. Use DUT 2 as the backup in the VRRP group and use DUT 1 as the master by configuring different priorities for them.
2. Specify the source IP address of BFD echo packets. As a best practice, specify the IP address of the loopback interface as the source IP address.
3. Create a track entry associated with the echo-mode BFD session. The remote IP address is the IP address of interface Port2 on DUT 2, and the local IP address is the IP address of interface Port1 on DUT 1.
4. Display BFD session information on DUT 1. Result 1 is expected.
5. Associate VRRP group 1 with a track entry.
6. Display VRRP group state information on DUT 1. Result 2 is expected.
7. Power down DUT 1. Result 3 is expected on DUT 1.

Expect Results:

1. An echo-mode BFD session is established and is in up state.
2. The output shows DUT 2 as the backup in the VRRP group, the track entry associated with the VRRP group, and the Switchover mode.
3. The log message about BFD session down is printed. DUT 2 changes from the backup to the master immediately, without waiting for three VRRP advertisement intervals.



19413/844594=0.02298 s=22.99 us

Actual Result：

1. Configuration on DUTs

DUT1

```
#
vlan 10
#
interface Vlan-interface10
 ip address 10.1.1.1 255.255.255.0
 vrrp vrid 1 virtual-ip 10.1.1.10
 vrrp vrid 1 priority 120
 vrrp vrid 1 track 1 priority reduced 50
 bfd min-echo-receive-interval 100
 bfd detect-multiplier 3
 bfd echo enable
#
 bfd echo-source-ip 10.10.10.10
#
track 2 bfd echo interface Vlan-interface10 remote ip 10.1.1.2 local ip 10.1.1.1
#
```

DUT2

```
#
 bfd echo-source-ip 20.20.20.20
#
track 1 bfd echo interface Vlan-interface10 remote ip 10.1.1.1 local ip 10.1.1.2
#
```

2. Display BFD session information on DUT 1.

```
[5560-2]dis bfd session
 Total Session Num: 1     Up Session Num: 1     Init Mode: Active

 IPv4 session working in echo mode:

 LD              SourceAddr      DestAddr        State    Holdtime    Interface
 129             10.1.1.2        10.1.1.1        Up       230ms       Vlan10
```

3. Associate VRRP group 1 with a track entry.

track 1 bfd echo int vlan 10 remote ip 10.1.1.1 local ip 10.1.1.2

4. Display VRRP group state information on DUT 1. Result 2 is expected.

```
[5560x-ei-1]dis vrrp verbose
IPv4 Virtual Router Information:
 Running mode : Standard
 Total number of virtual routers : 1
   Interface Vlan-interface10
     VRID              : 1                 Adver Timer   : 100
     Admin Status      : Up                State         : Master
     Config Pri        : 120               Running Pri   : 120
     Preempt Mode      : Yes               Delay Time    : 0
     Auth Type         : Not supported
     Version           : 3
     Virtual IP        : 10.1.1.10
     Virtual MAC       : 0000-5e00-0101
     Master IP         : 10.1.1.1
   VRRP Track Information:
     Track Object    : 1                 State : Positive    Pri Reduced : 50

[5560x-ei-1]
```

```
<5560x-ei-1>reboot
Start to check configuration with next startup configuration file, please wait.........DONE!
This command will reboot the device. Continue? [Y/N]:y
```

4. An echo-mode BFD session is established and is in up state.

```
[5560-2]dis bfd session
 Total Session Num: 1     Up Session Num: 1     Init Mode: Active

 IPv4 session working in echo mode:

 LD              SourceAddr      DestAddr        State    Holdtime    Interface
 129             10.1.1.2        10.1.1.1        Up       230ms       Vlan10
```

5. The output shows DUT 2 as the backup in the VRRP group, the track entry associated with the VRRP group, and the Switchover mode.

```
[5560-2]dis vrrp verbose
IPv4 Virtual Router Information:
 Running mode : Standard
 Total number of virtual routers : 1
   Interface Vlan-interface10
     VRID              : 1                 Adver Timer   : 100
     Admin Status      : Up                State         : Backup
     Config Pri        : 100               Running Pri   : 100
     Preempt Mode      : Yes               Delay Time    : 0
     Become Master     : 2630ms left
     Auth Type         : None
     Virtual IP        : 10.1.1.10
     Virtual MAC       : 0000-5e00-0101
     Master IP         : 10.1.1.1
   VRRP Track Information:
     Track Object    : 1                 State : Positive   Switchover

[5560-2]
```

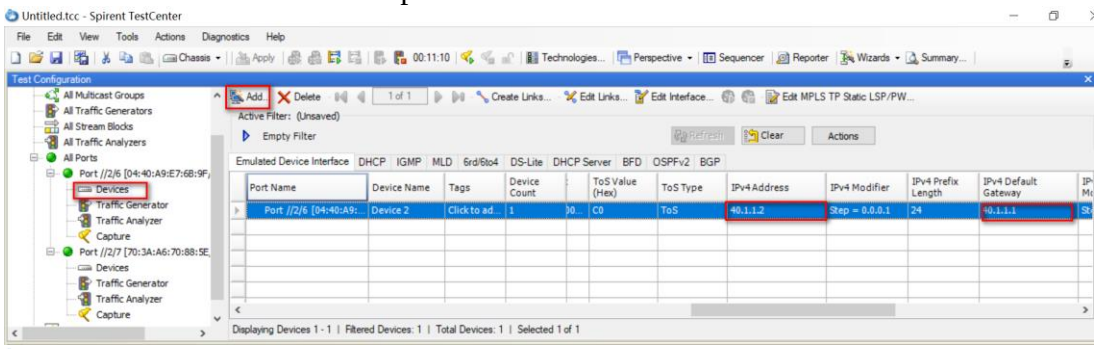
6. The log message about BFD session down is printed. DUT 2 changes from the backup to the master immediately, without waiting for three VRRP advertisement intervals.

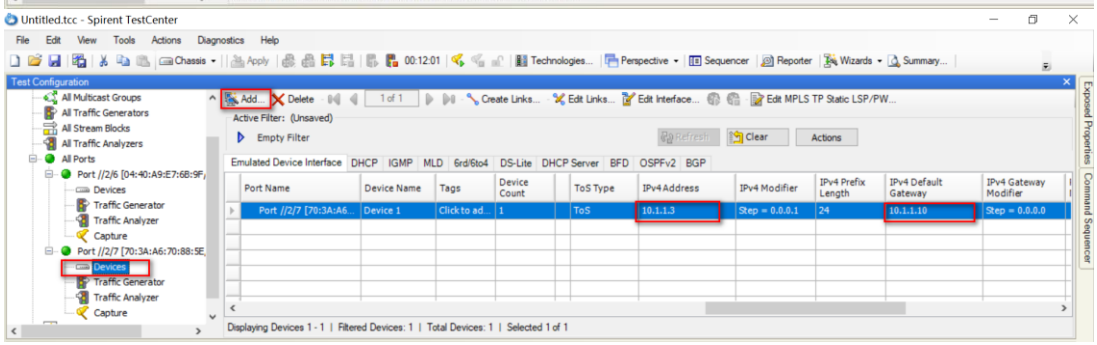
```
[5560x-ei-1]int vl 10
[5560x-ei-1-Vlan-interface10]shu
[5560x-ei-1-Vlan-interface10]%Jan 25 10:44:58:169 2021 5560x-ei-1 VRRP4/6/VRRP_STATUS_CHANGE: Th
e status of IPv4 virtual router 1 (configured on Vlan-interface10) changed from Master to Initia
lize: Interface event received.
%Jan 25 10:44:58:192 2021 5560x-ei-1 BFD/5/BFD_CHANGE_FSM: Sess[10.1.1.1/10.1.1.2, LD/RD:130/130
, Interface:Vlan10, SessType:Echo, LinkType:INET], Ver:1, Sta: UP->DOWN, Diag: 2 (Echo Function
Failed)
%Jan 25 10:44:58:198 2021 5560x-ei-1 TRACK/6/TRACK_STATE_CHANGE: The state of track entry 2 chan
ged from Positive to Negative.
%Jan 25 10:44:58:201 2021 5560x-ei-1 IFNET/3/PHY_UPDOWN: Physical state on the interface Vlan-in
terface10 changed to down.
%Jan 25 10:44:58:202 2021 5560x-ei-1 IFNET/5/LINK_UPDOWN: Line protocol state on the interface V
lan-interface10 changed to down.

dis bfd se
 Total Session Num: 1     Up Session Num: 0     Init Mode: Active

 IPv4 session working in echo mode:

 LD            SourceAddr      DestAddr        State    Holdtime    Interface
 130           10.1.1.1        10.1.1.2        Down       /         Vlan10
[5560x-ei-1-Vlan-interface10]
```

```
IPv4 Virtual Router Information:
 Running mode : Standard
 Total number of virtual routers : 1
   Interface Vlan-interface10
     VRID              : 1                 Adver Timer   : 100
     Admin Status      : Up                State         : Initialize
     Config Pri        : 120               Running Pri   : 120
     Preempt Mode      : Yes               Delay Time    : 0
     Auth Type         : Not supported
     Version           : 3
     Virtual IP        : 10.1.1.10
     Master IP         : 0.0.0.0
   VRRP Track Information:
     Track Object    : 1                 State : NotReady   Pri Reduced : 50

[5560x-ei-1-Vlan-interface10]
```

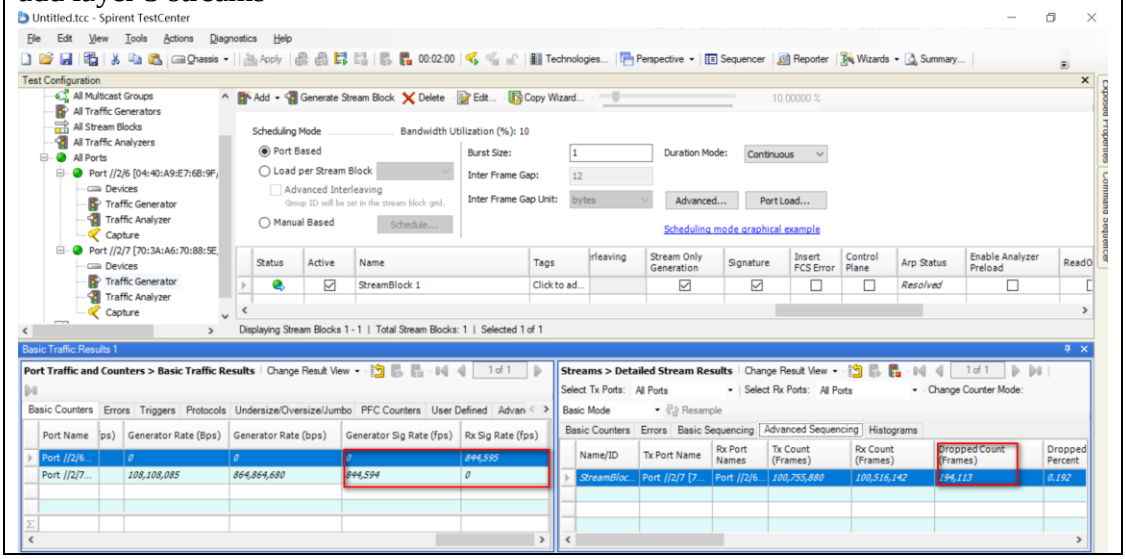
```
IPv4 Virtual Router Information:
 Running mode : Standard
 Total number of virtual routers : 1
   Interface Vlan-interface10
     VRID              : 1                 Adver Timer   : 100
     Admin Status      : Up                State         : Master
     Config Pri        : 100               Running Pri   : 100
     Preempt Mode      : Yes               Delay Time    : 0
     Auth Type         : None
     Virtual IP        : 10.1.1.10
     Virtual MAC       : 0000-5e00-0101
     Master IP         : 10.1.1.2
   VRRP Track Information:
     Track Object    : 1                 State : Negative   Switchover

<5560-2>
<5560-2>
```

add devices on both two tester ports





add layer 3 streams



19413/844594=0.02298 s=22.99 us

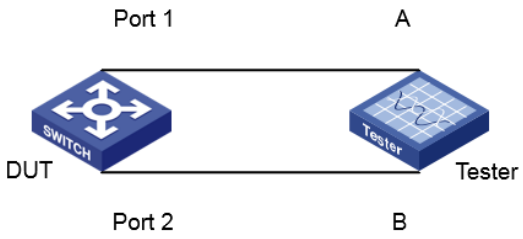
7. Details for DUTs configurations

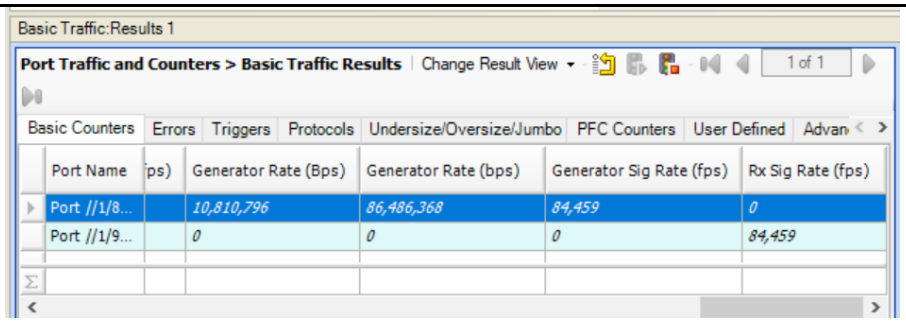
DUT1

DUT2

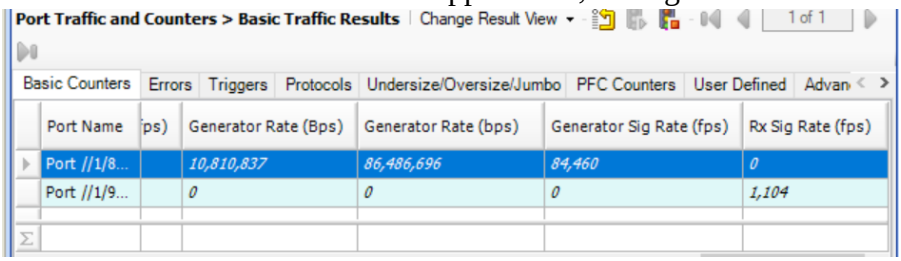
☐ Passed	☐ Failed

3.5 Broadcast Suppression

Test Item Name: Broadcast Suppression
Work Hour：10 min
Test Topology: 
Test Process: 1. Create Stream1: broadcast, 1G 2. Send the Stream1 from the Port A, with expected Result 1 3. Configure the broadcast suppression 1024pps on the Port 1 4. Send the Stream1 from the Port A, with expected Result 2
Expect Results: 1. Tester Port B receive the 1G traffic

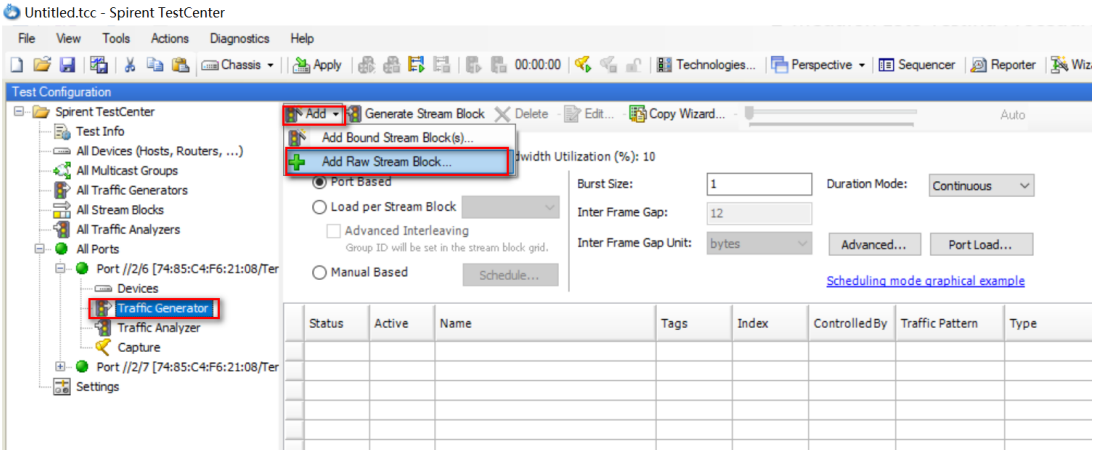


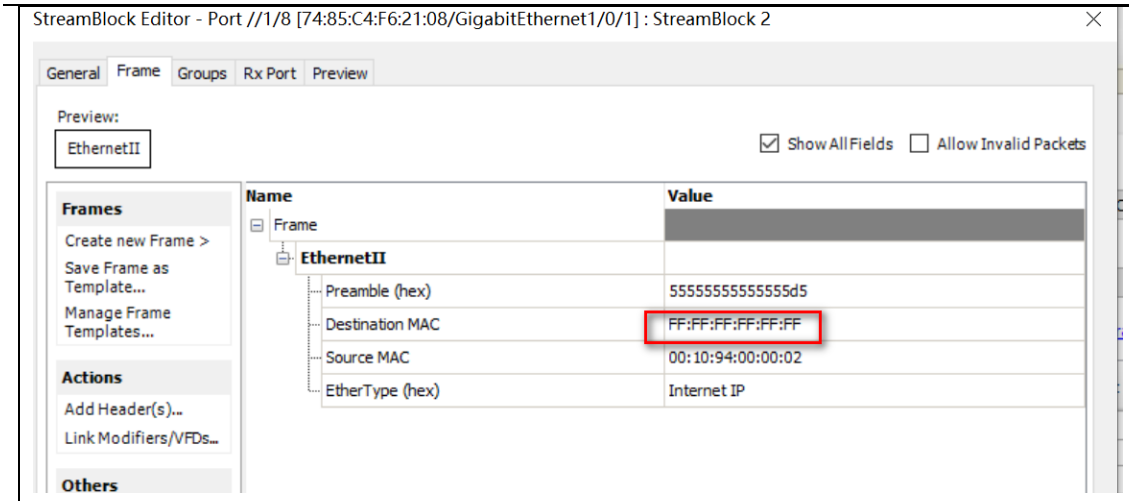
2. Tester Port B receive the 1024pps traffic, average error is less than 1%.



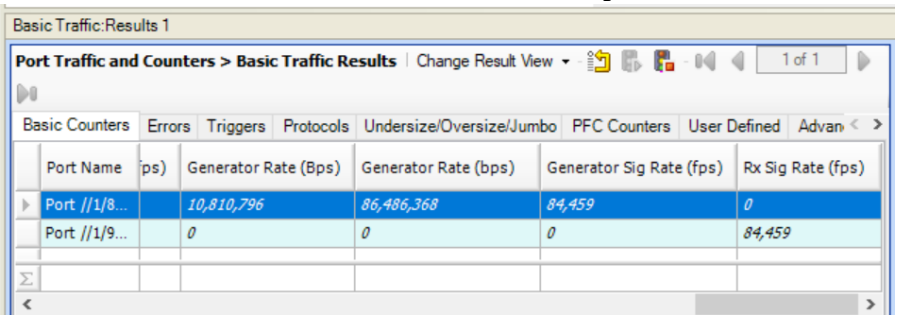
Actual Result：

1. Create Stream1: broadcast, 1G





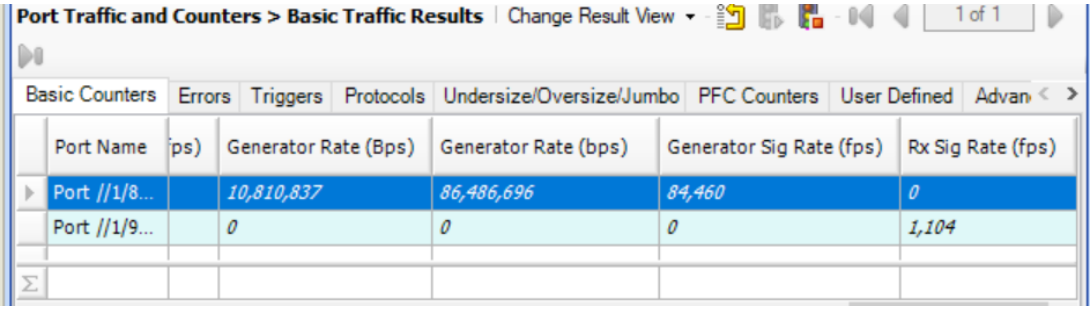
2. Send the Stream1 from the Port A, with expected Result 1



3. Configure the broadcast suppression 1024pps on the Port 1

```
[5560x-ei-1-GigabitEthernet1/0/2]int g1/0/1
[5560x-ei-1-GigabitEthernet1/0/1]br
[5560x-ei-1-GigabitEthernet1/0/1]broadcast-suppression p
[5560x-ei-1-GigabitEthernet1/0/1]broadcast-suppression pps 1024
```

4. Send the Stream1 from the Port A.



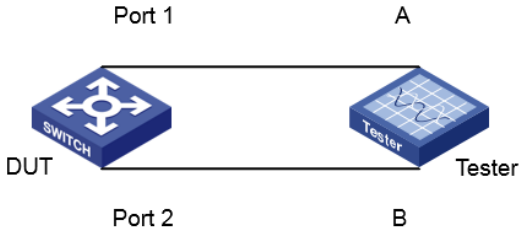
☐ Passed	☐ Failed

3.6 Multicast Suppression

Test Item Name: Multicast Suppression

Work Hour: 20 min

Test Topology:



Test Process:

1. Create Stream1: multicast, 1G.
2. Send the Stream1 from the Port A, with expected Result 1.
3. Configure the multicast suppression 1024pps on the Port 1.
4. Send the Stream1 from the Port A, with expected Result 2.

Expect Results:

1. Tester Port B receive the 1G traffic.
2. Tester Port B receive the 1024pps traffic, average error is less than 1%.

Actual Result：

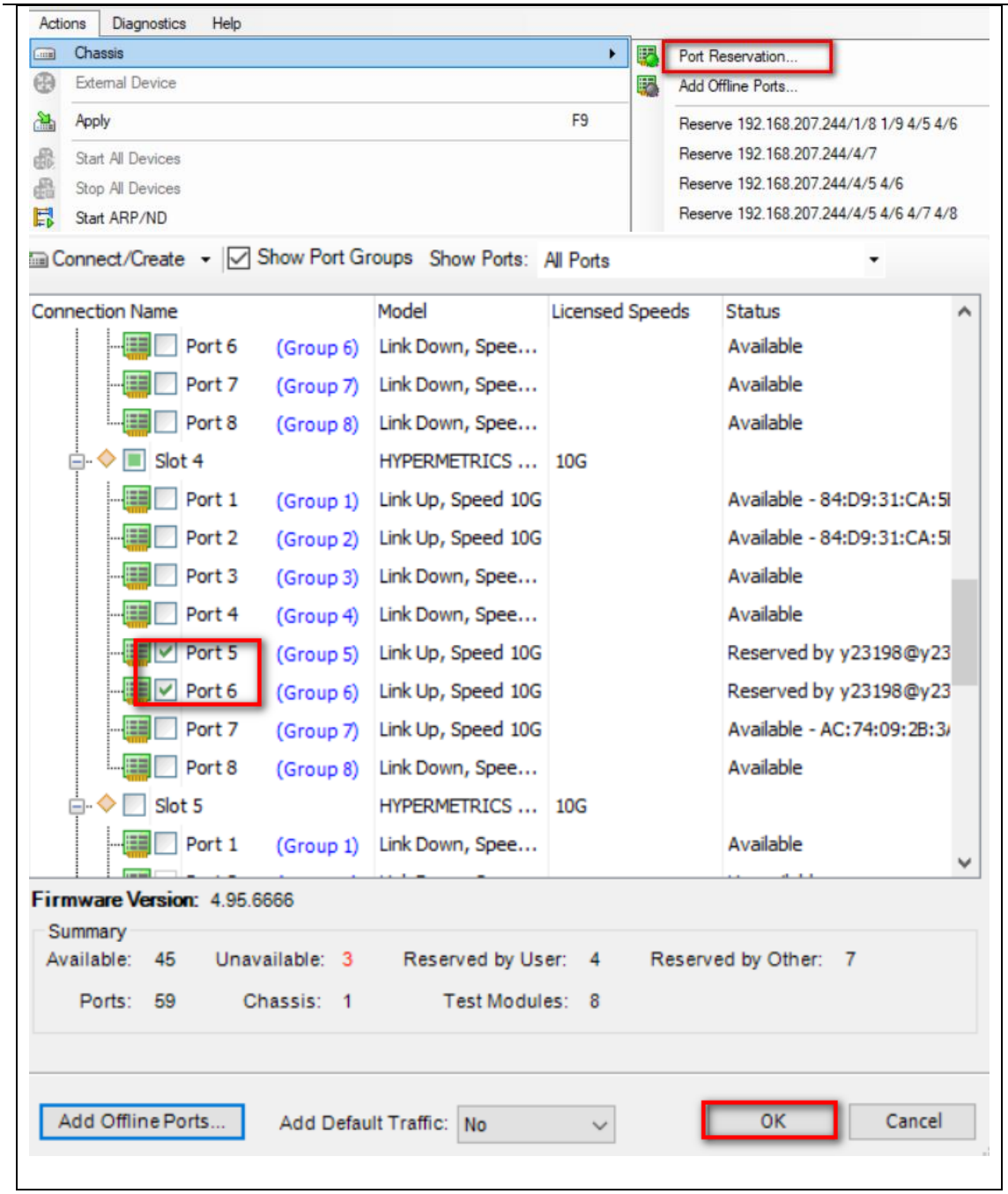
1. Enable igmp-snooping globally and on vlan 100

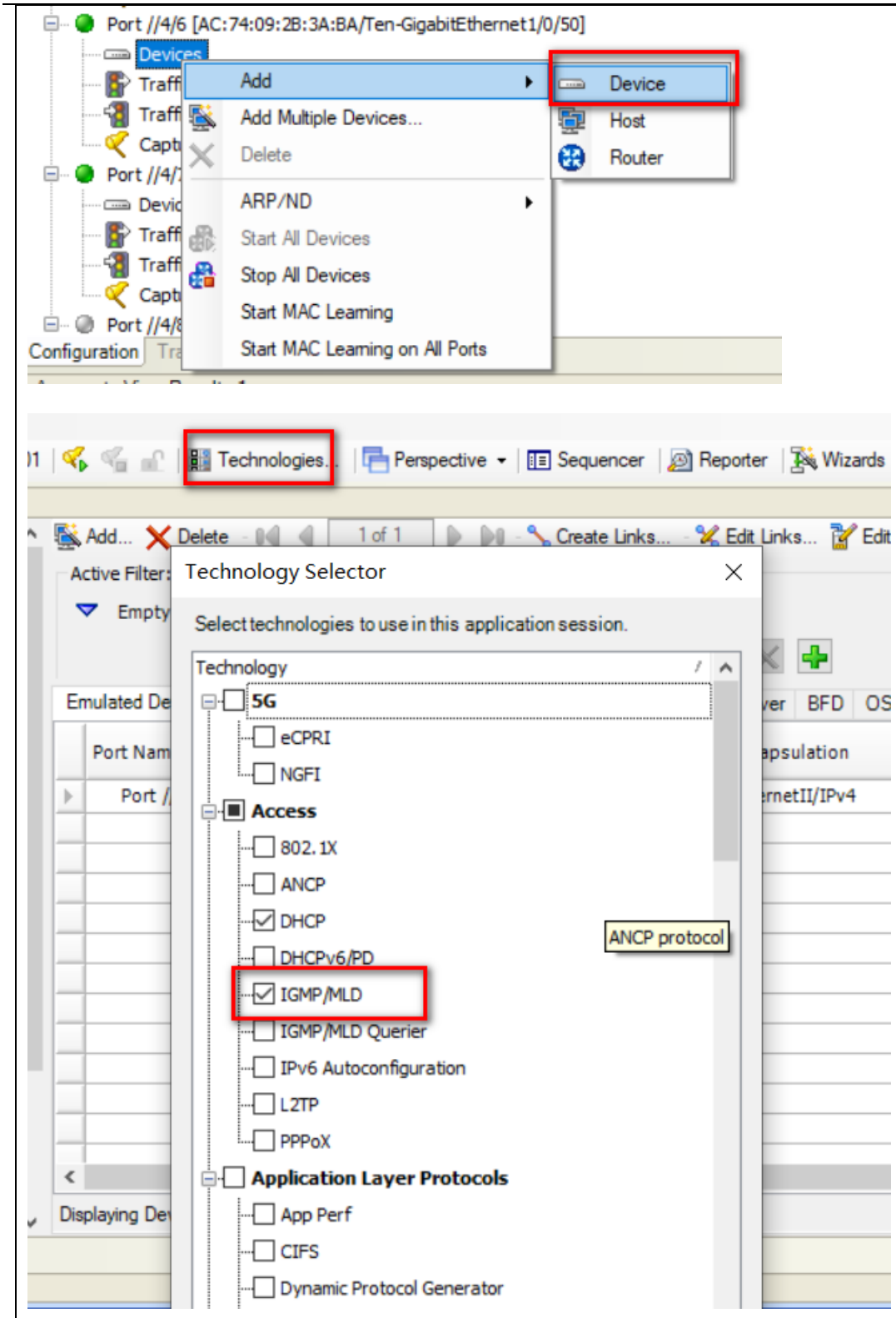
```
[DUT]igmp-snooping
[DUT-igmp-snooping]quit
[DUT]vlan 100
[DUT-vlan100]igmp-snooping enable
```

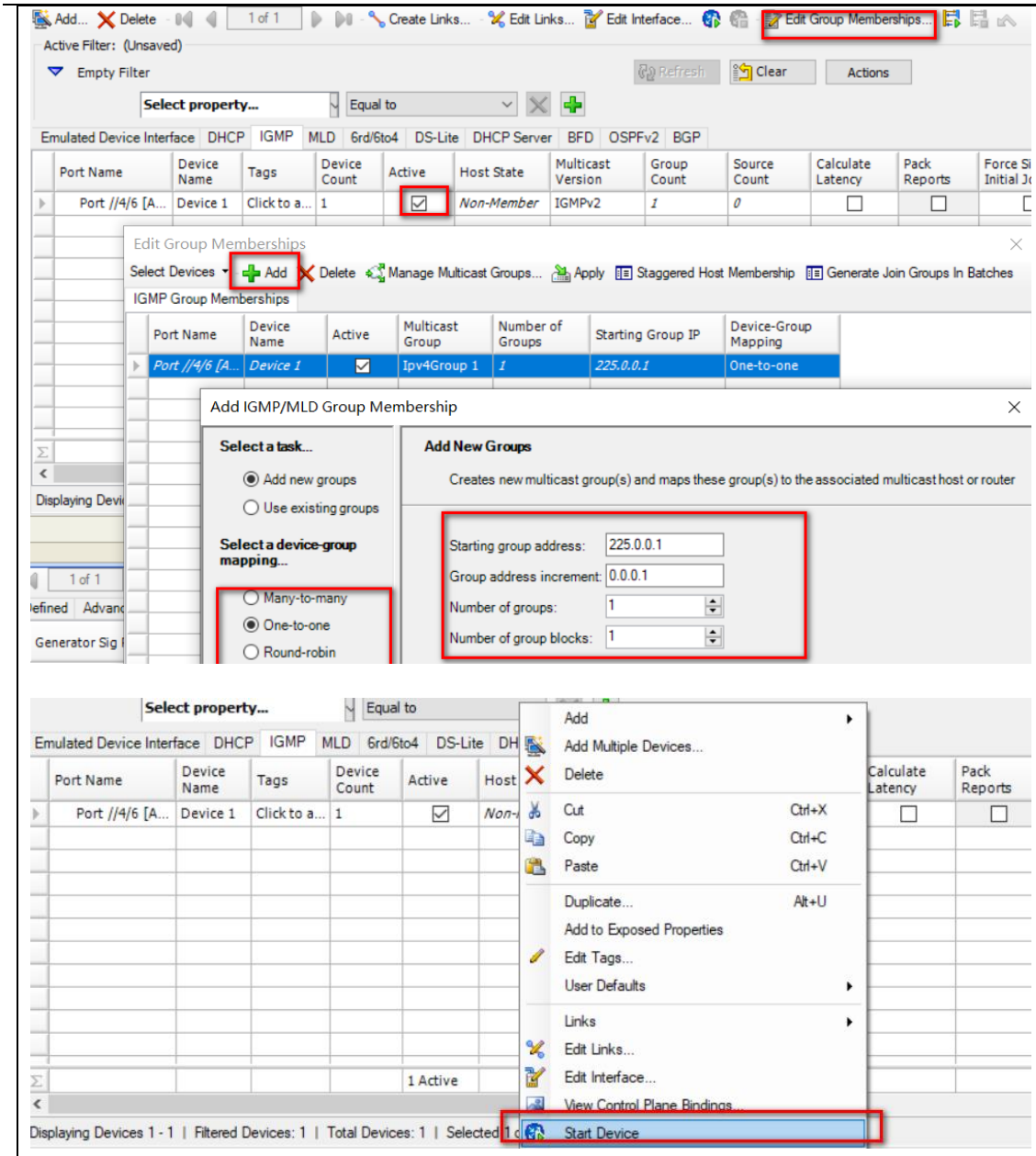
2. Create VLAN 100, assign Port A/B of DUT to join VLAN 100

```
[DUT-vlan100]port Ten-GigabitEthernet 1/0/49
[DUT-vlan100]port Ten-GigabitEthernet 1/0/50
```

3. The DUT Port B is configured with igmp-snooping static-group 225.0.0.1 vlan 100



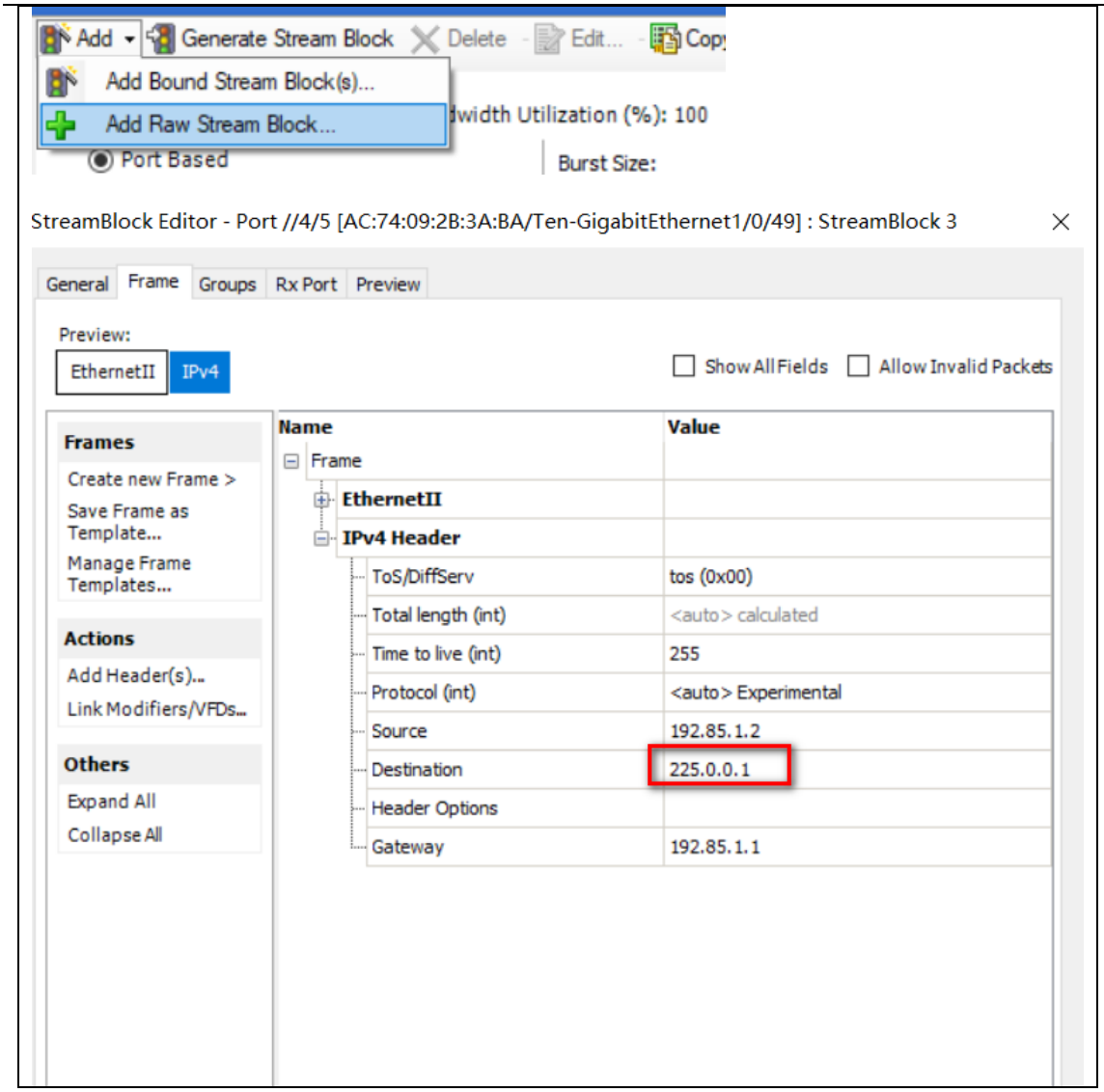


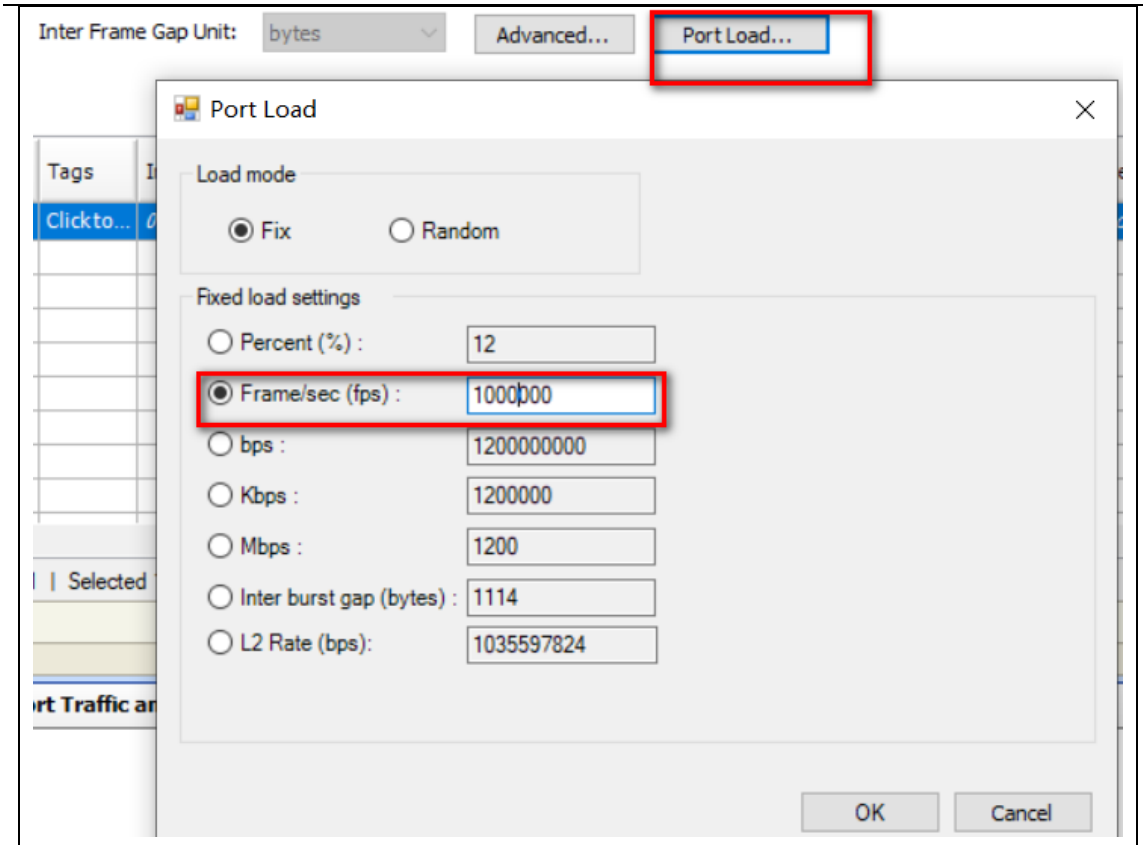


4. DUT display igmp-snooping static-group

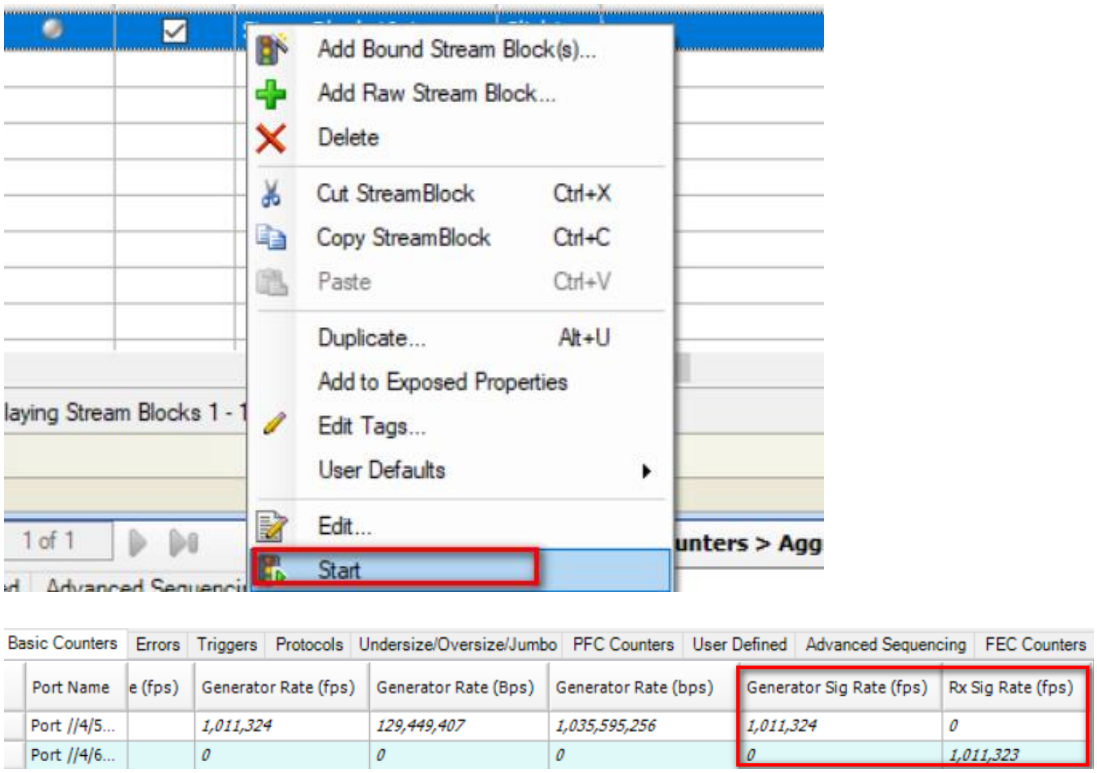
```
[DUT]dis igmp-snooping group
Total 1 entries.

VLAN 100: Total 1 entries.
  (0.0.0.0, 225.0.0.1)
    Host ports (1 in total):
      XGE1/0/50                                (00:04:18)
[DUT]
```

5. Send the destination IP 225.0.0.1 into port A of tester, load is 1G





6. Start traffic, result 1 is expected



7. Configure the multicast suppression 1000pps on the Port 1, result 2 is expected.

```
[DUT-Ten-GigabitEthernet1/0/49]multicast-suppression pps 1000
```

Port Name	e (fps)	Generator Rate (fps)	Generator Rate (Bps)	Generator Rate (bps)	Generator Sig Rate (fps)	Rx Sig Rate (fps)
Port //4/5...		1,011,324	129,449,425	1,035,595,400	1,011,324	0
Port //4/6...		0	0	0	0	1,000

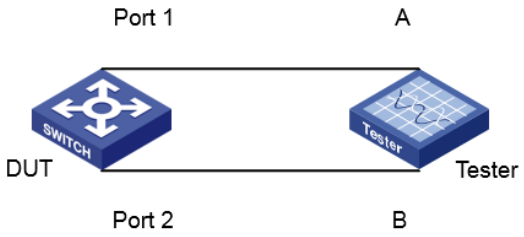
☐ Passed	☐ Failed

3.7 Unicast Suppression

Test Item Name: unicast Suppression

Work Hour: 20 min

Test Topology:



Test Process:

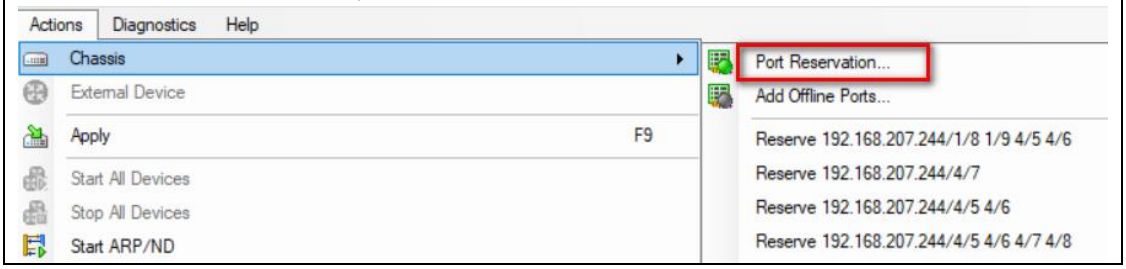
1. Create Stream1: unicast, 1G.
2. Send the Stream1 from the Port A, with expected Result 1.
3. Configure the unicast suppression 1024pps on the Port 1.
4. Send the Stream1 from the Port A, with expected Result 2.

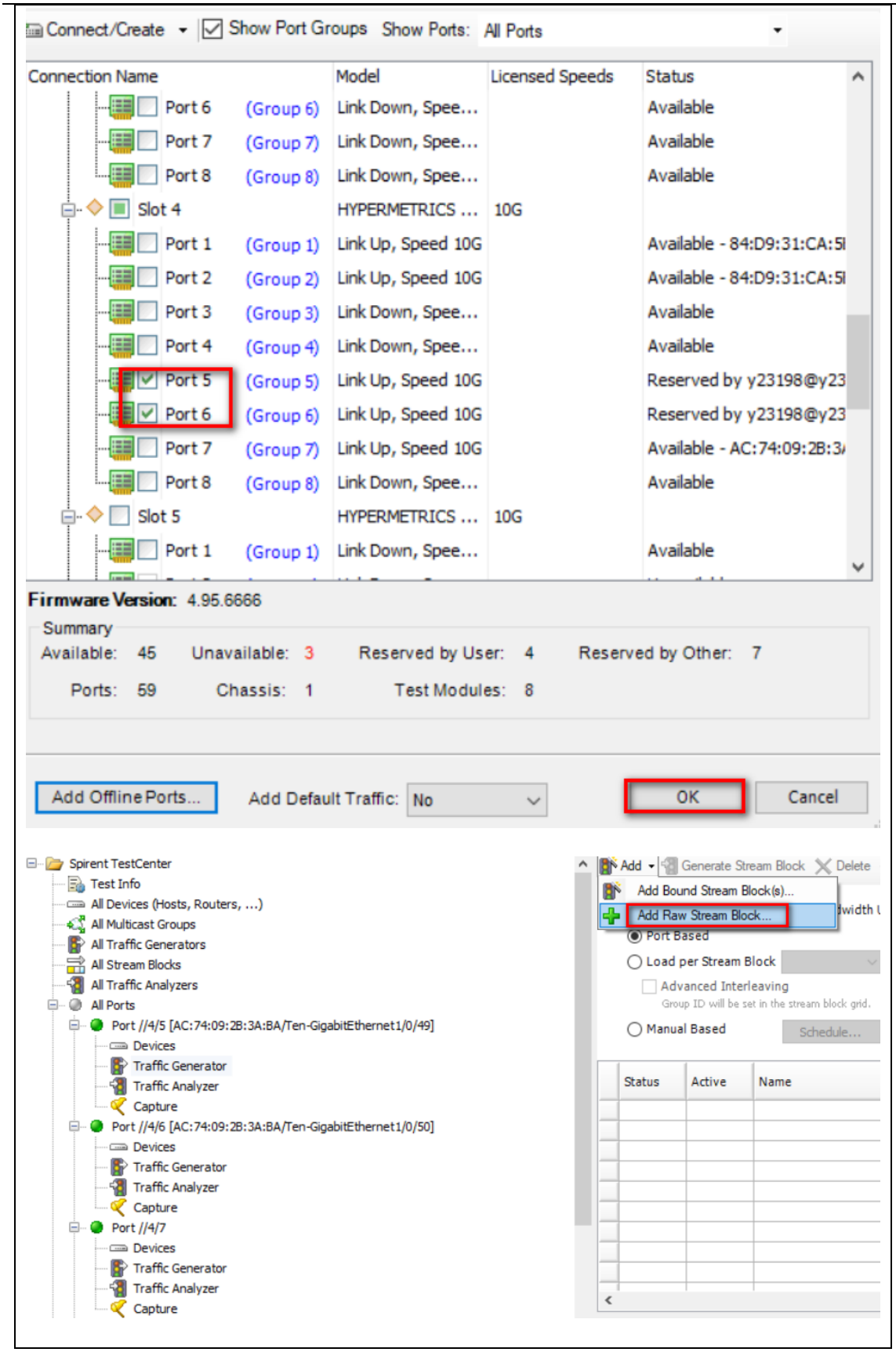
Expect Results:

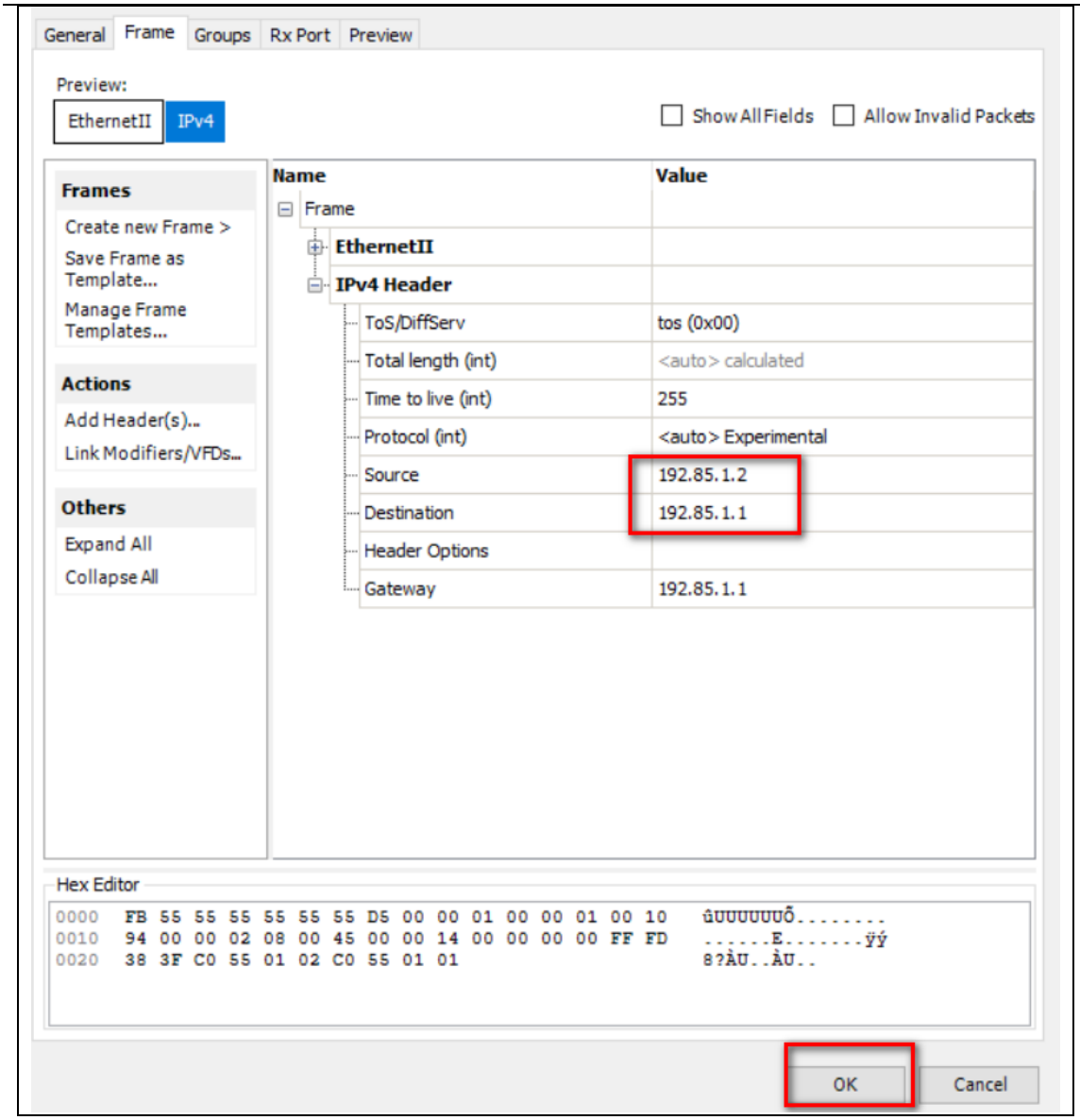
1. Tester Port B receive the 1G traffic.
2. Tester Port B receive the 1024pps traffic, average error is less than 1%.

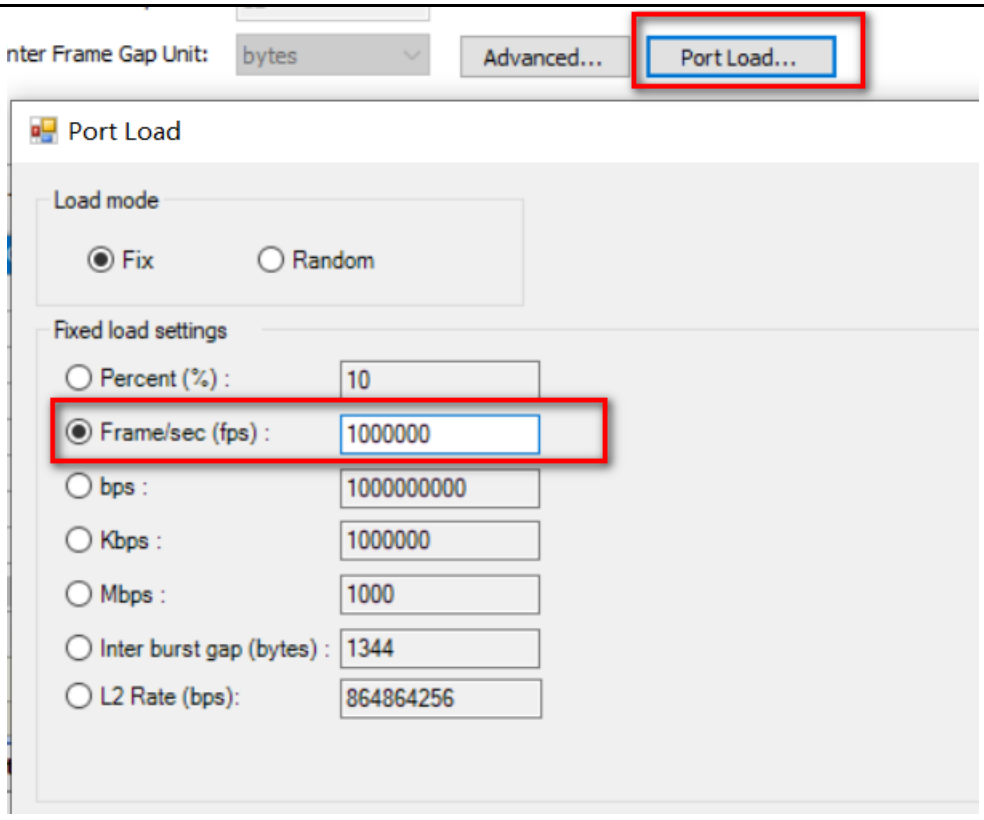
Actual Result:

1. Create unicast stream, the load is 1G

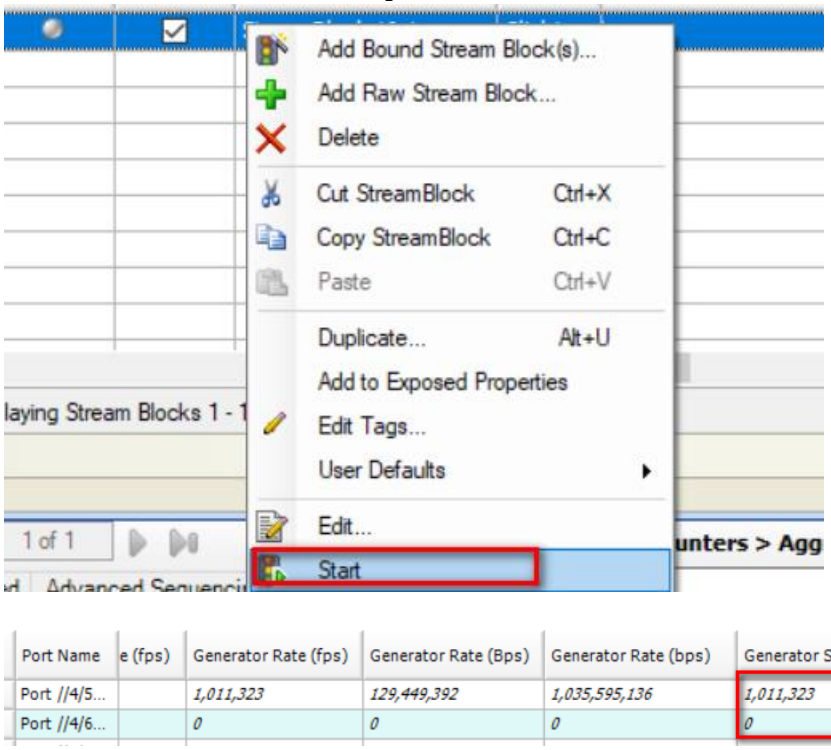








2. Start traffic, result 1 is expected



Port Name	e (fps)	Generator Rate (fps)	Generator Rate (Bps)	Generator Rate (bps)	Generator Sig Rate (fps)	Rx Sig Rate (fps)
Port //4/5...		1,011,323	129,449,392	1,035,595,136	1,011,323	0
Port //4/6...		0	0	0	0	1,011,323

3. Configure the unicast suppression 1000pps on the Port 1, result 2 is expected

```
[DUT-Ten-GigabitEthernet1/0/49]unicast-suppression pps 1000
```

Port Name	e (fps)	Generator Rate (fps)	Generator Rate (Bps)	Generator Rate (bps)	Generator Sig Rate (fps)	Rx Sig Rate (fps)
Port //4/5...		1,011,323	129,449,401	1,035,595,208	1,011,323	0
Port //4/6...		0	0	0	0	1,000

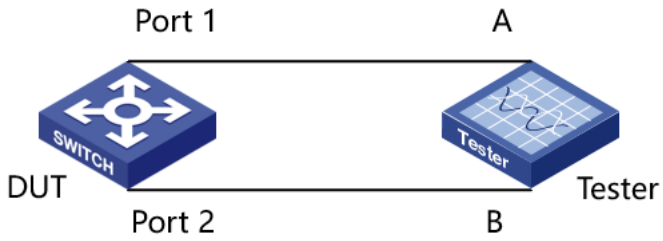
☐ Passed	☐ Failed

3.8 IGMP V1/V2/V3

Test Item Name: IGMP V1/V2/V3

Work Hour:30 min

Test Topology:



Test Process:

1. Create VLAN 2, assign Port 1 to the VLAN. Create VLAN 3, assign Port 2 to the VLAN.
2. Configure IP address for layer 3 virtual interface of VLAN 2 and VLAN 3, Port A of Tester and layer 3 virtual interface in the same segment.
3. Enable IGMP in Vlan-interface3 interface view, set up IGMP version 1, enable PIM DM in all ports:
4. Send multicast data of 225.0.0.1 from Port A of Tester to DUT, source address is the port A address of Tester. Result 1 is expected.
5. Send an IGMP message from Port B of Tester to simulate joining multicast group 225.0.0.1. Result 2 is expected.
6. Enable IGMP in Vlan-interface3 interface view, set up IGMP version 2, enable pim dm in all ports:
7. Send multicast data of 225.0.0.1 from Port A of Tester to DUT. Result 1 is expected.
8. Send an IGMP message from Port B of Tester to simulate joining multicast group 225.0.0.1. Result 2 is expected.

9. Send an IGMP message from Port B of Tester to simulate leaving multicast group 225.0.0.1. Result 1 is expected.
10. Enable IGMP in Vlan-interface3 interface view, set up IGMP version 3, enable PIM DM in all layer 3 ports:：
11. Send multicast data of 225.0.0.1 from Port A of Tester to DUT, source address is the port A address of Tester. Result 1 is expected.
12. Send an IGMPv3 message from Port B of Tester to simulate joining multicast group IS_IN (A) of 225.0.0.1, A indicates the port A address of Tester. Result 3 is expected.
13. Tester port B leaves multicast group IS_IN（A）of 225.0.0.1. Result A is expected.
14. Send an IGMPv3 message from Port B of Tester to simulate joining multicast group IS_IN (not A) of 225.0.0.1. Result 4 is expected.

Expect Results:

1. Tester Port B doesn't receive multicast traffic；
2. Multicast group 225.0.0.1 joined, Tester Port B receives multicast data.
3. Multicast group 225.0.0.1 joined, Tester Port B receives multicast data.
4. Multicast group 225.0.0.1 joined, Tester Port B doesn't receive multicast data.

Actual Result：

1. Create VLAN 2, assign Port 1 to the VLAN. Create VLAN 3, assign Port 2 to the VLAN.

```
[DUT2]vlan 2
[DUT2-vlan2]port Ten-GigabitEthernet 1/0/49
```

```
[DUT2]vlan 3
[DUT2-vlan3]port Ten-GigabitEthernet 1/0/50
```

2. Configure IP address for layer 3 virtual interface of VLAN 2 and VLAN 3, Port A of Tester and layer 3 virtual interface in the same segment.

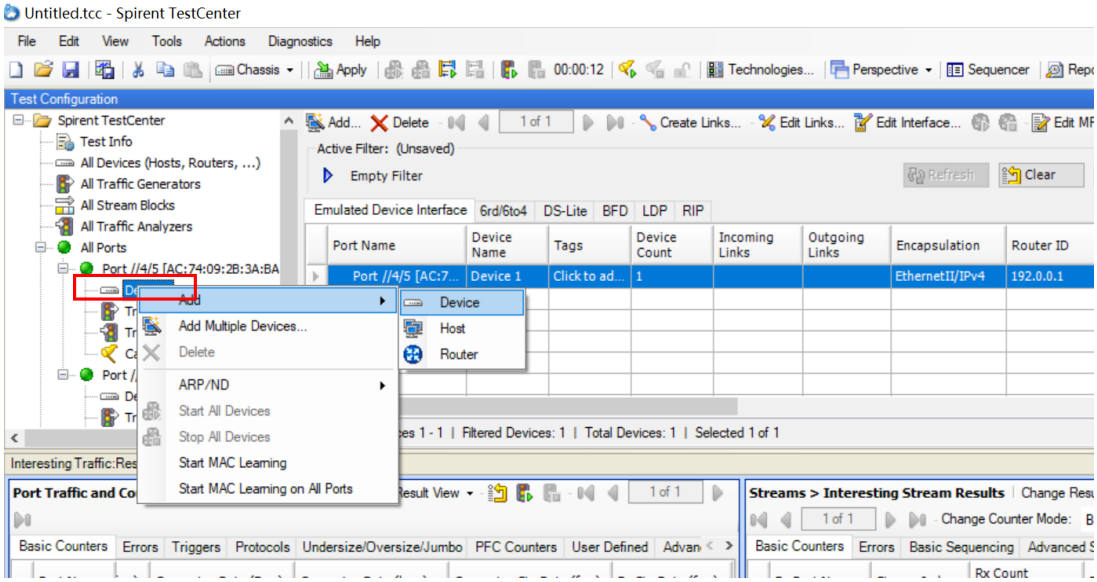
```
[DUT2]interface Vlan-interface 2
[DUT2-Vlan-interface2]ip address 20.1.1.1 24
```

```
[DUT2]interface Vlan-interface 3
[DUT2-Vlan-interface3]ip address 30.1.1.1 24
```

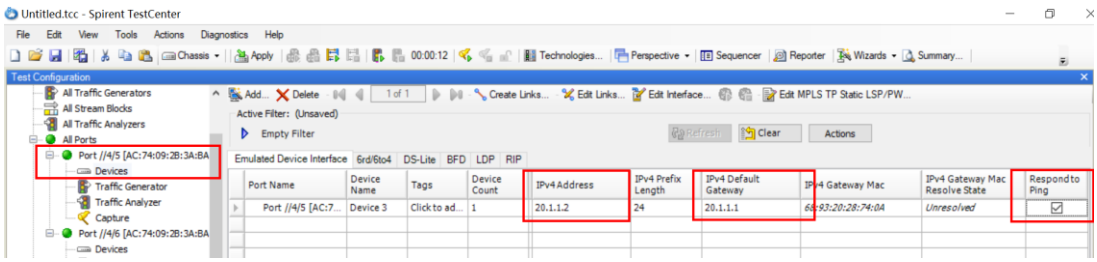
Create a device on each ports on the tester.

On Port 4/5:

Add a new device.

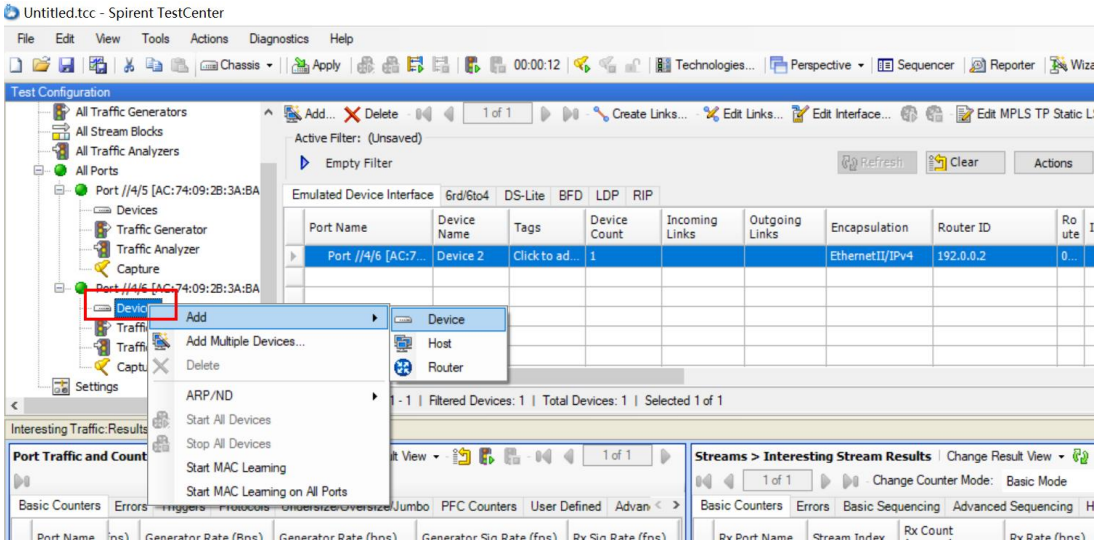


Set the ipv4 address and the gateway.

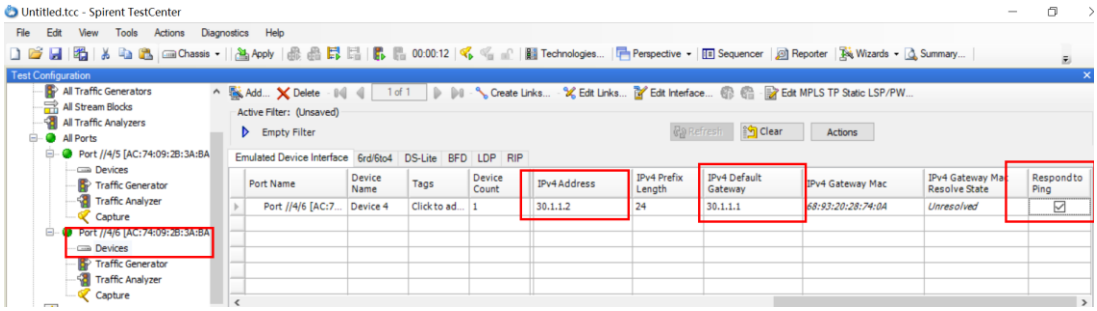


On Port 4/6:

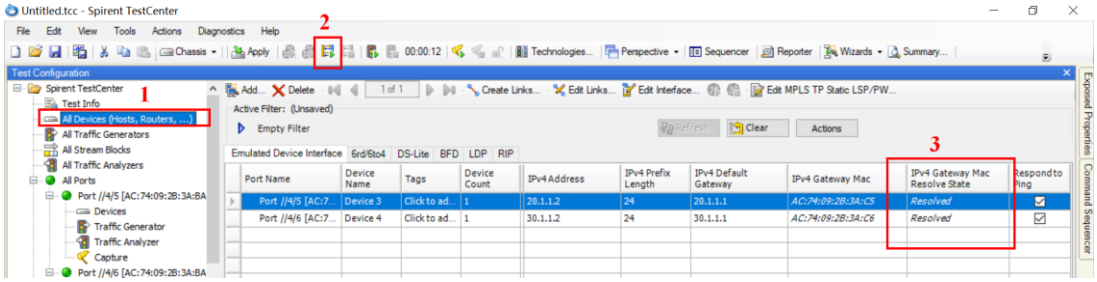
Add a new device:



Set the IPv4 address and the gateway.



Select devices configured on the port and use ARP to resolve the gateway Mac address;



3. Enable IGMP in Vlan-interface3 interface view, set up IGMP version 1, enable PIM DM in all ports:

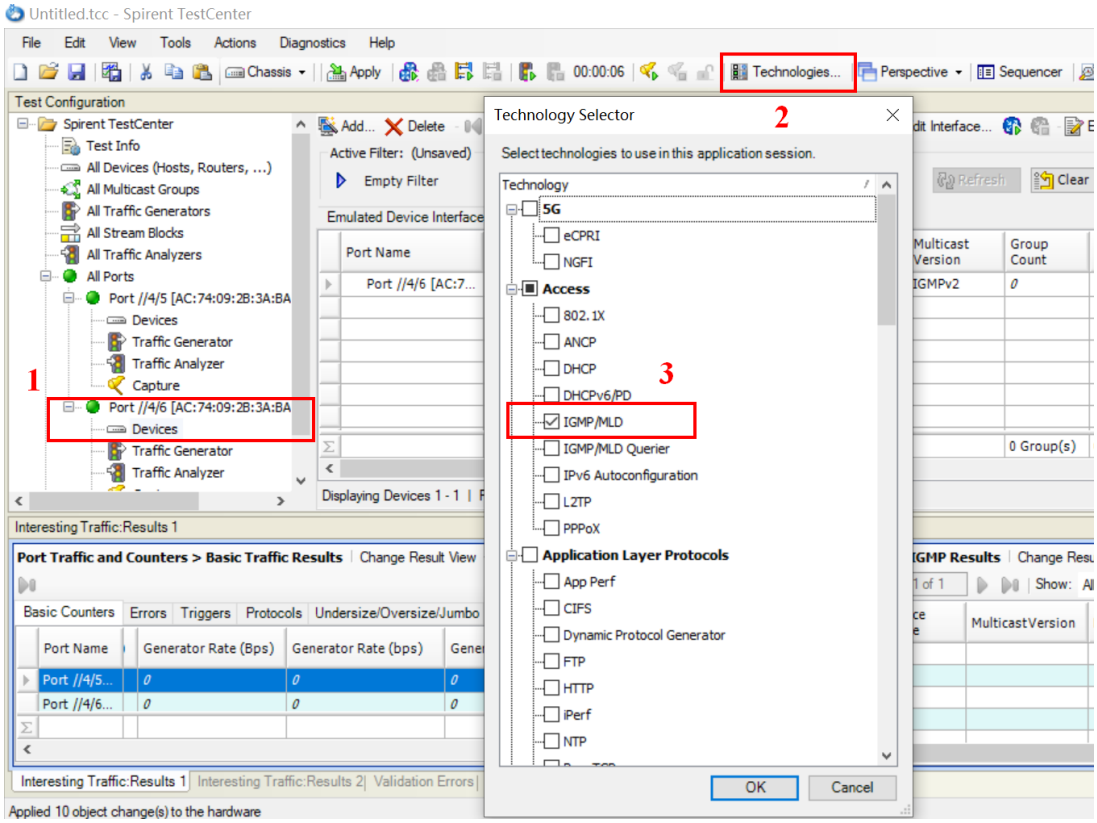
```
[DUT2]multicast routing
[DUT2-mrib]quit
```

```
[DUT2]interface Vlan-interface 3
[DUT2-Vlan-interface3]igmp enable
[DUT2-Vlan-interface3]igmp version 1
[DUT2-Vlan-interface3]pim dm
```

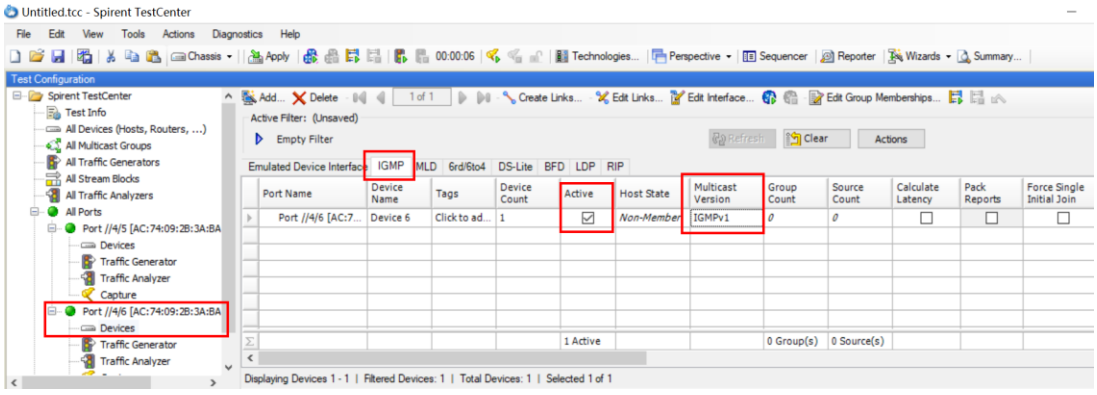
```
[DUT2]interface Vlan-interface 2
[DUT2-Vlan-interface2]pim dm
```

4. Send multicast data of 225.0.0.1 from Port A of Tester to DUT, source address is the port A address of Tester. Result 1 is expected.

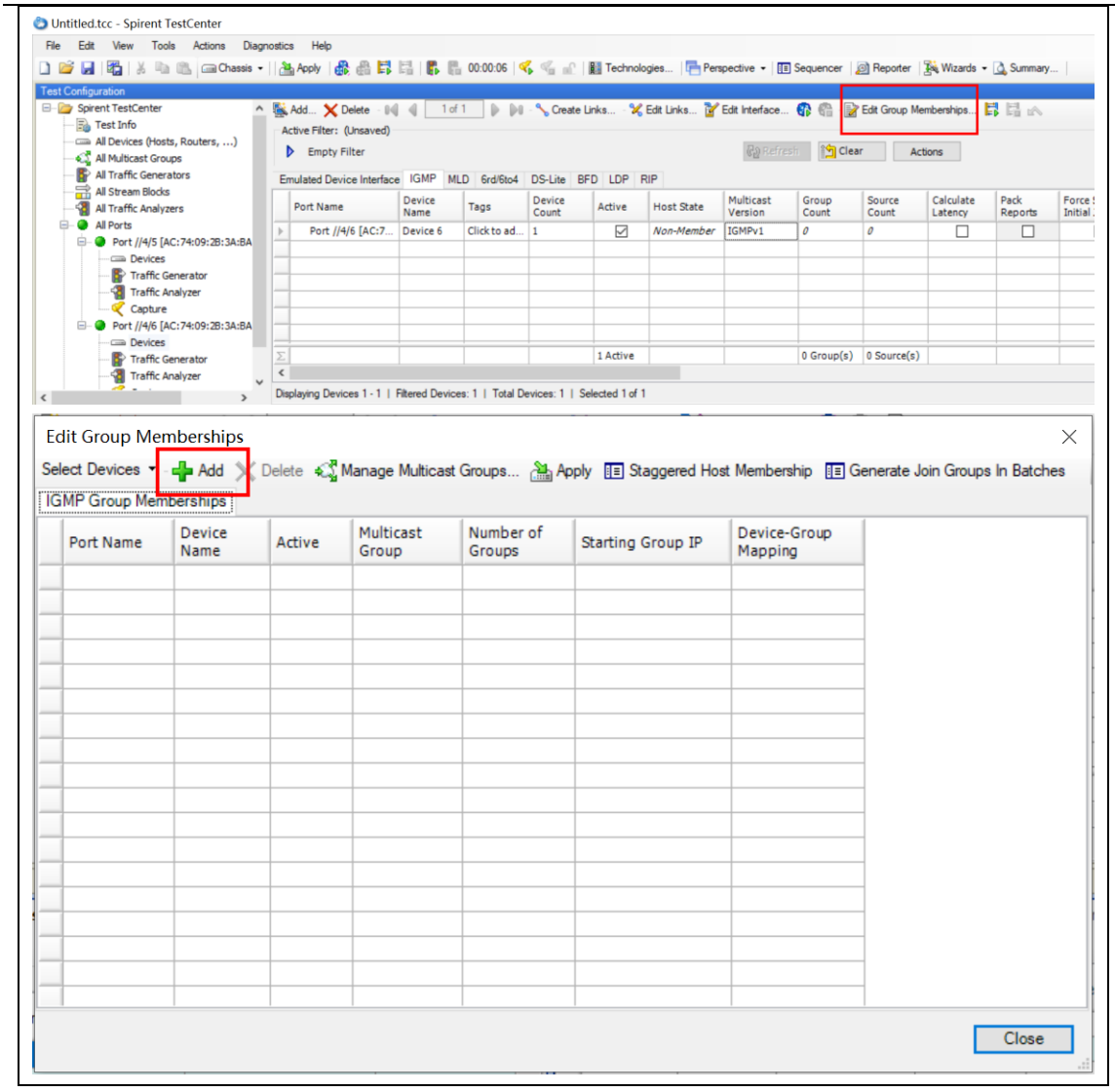
Select to use the IGMP protocol

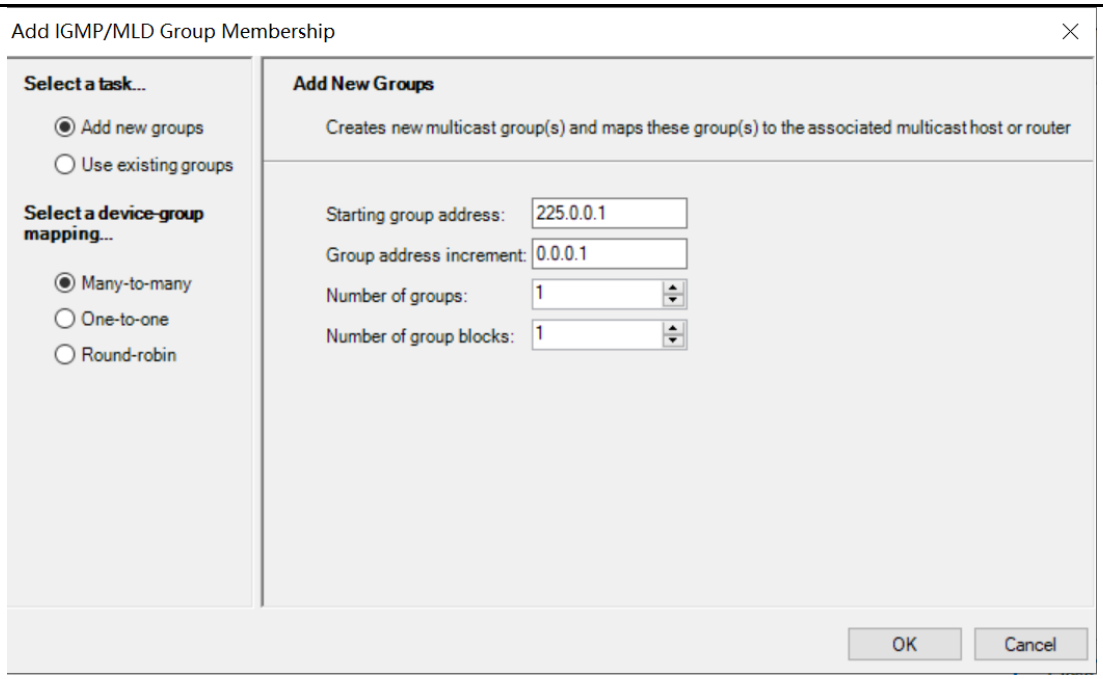


Select the multicast receiver Port 4/6, select it in the "Active" box, and the default version of IGMP is v1



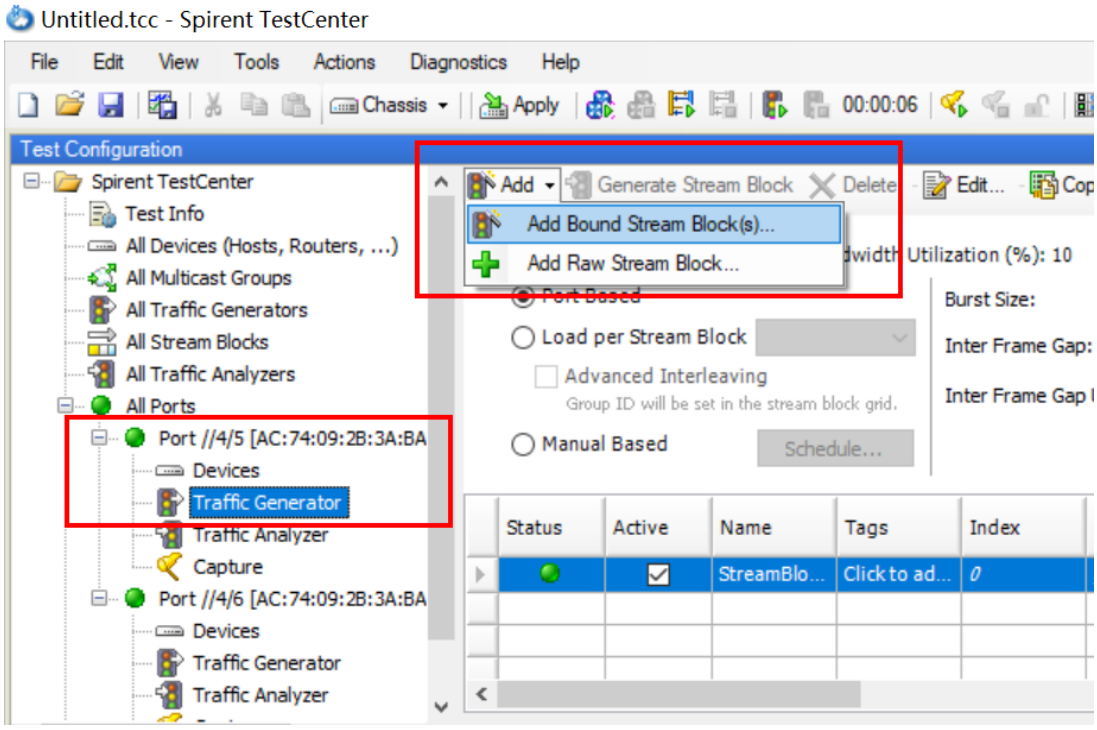
Add multicast group members.


Untitled.tcc - Spirent TestCenter
File Edit View Tools Actions Diagnostics Help
Test Configuration
Spirent TestCenter
Test Info
All Devices (Hosts, Routers, ...)
All Multicast Groups
All Traffic Generators
All Stream Blocks
All Traffic Analyzers
All Ports
Port //4/5 [AC:74:09:2B:3A:BA
Devices
Traffic Generator
Traffic Analyzer
Capture
Port //4/6 [AC:74:09:2B:3A:BA
Devices
Traffic Generator
Traffic Analyzer
Add... Delete 1 of 1 Create Links... Edit Links... Edit Interface... Edit Group Memberships...
Active Filter: (Unsaved)
Empty Filter
Refresh Clear Actions
Emulated Device Interface IGMP MLD 6rd/6to4 DS-Lite BFD LDP RIP
Port Name
Device Name
Tags
Device Count
Active
Host State
Multicast Version
Group Count
Source Count
Calculate Latency
Pack Reports
Force Initial
Port //4/6 [AC:7...
Device 6
Click to ad...
1
Non-Member
IGMPv1
0
0
1 Active
0 Group(s)
0 Source(s)
Displaying Devices 1 - 1 | Filtered Devices: 1 | Total Devices: 1 | Selected 1 of 1
Edit Group Memberships
Select Devices
Add
Delete
Manage Multicast Groups...
Apply
Staggered Host Membership
Generate Join Groups In Batches
IGMP Group Memberships
Port Name
Device Name
Active
Multicast Group
Number of Groups
Starting Group IP
Device-Group Mapping
Close

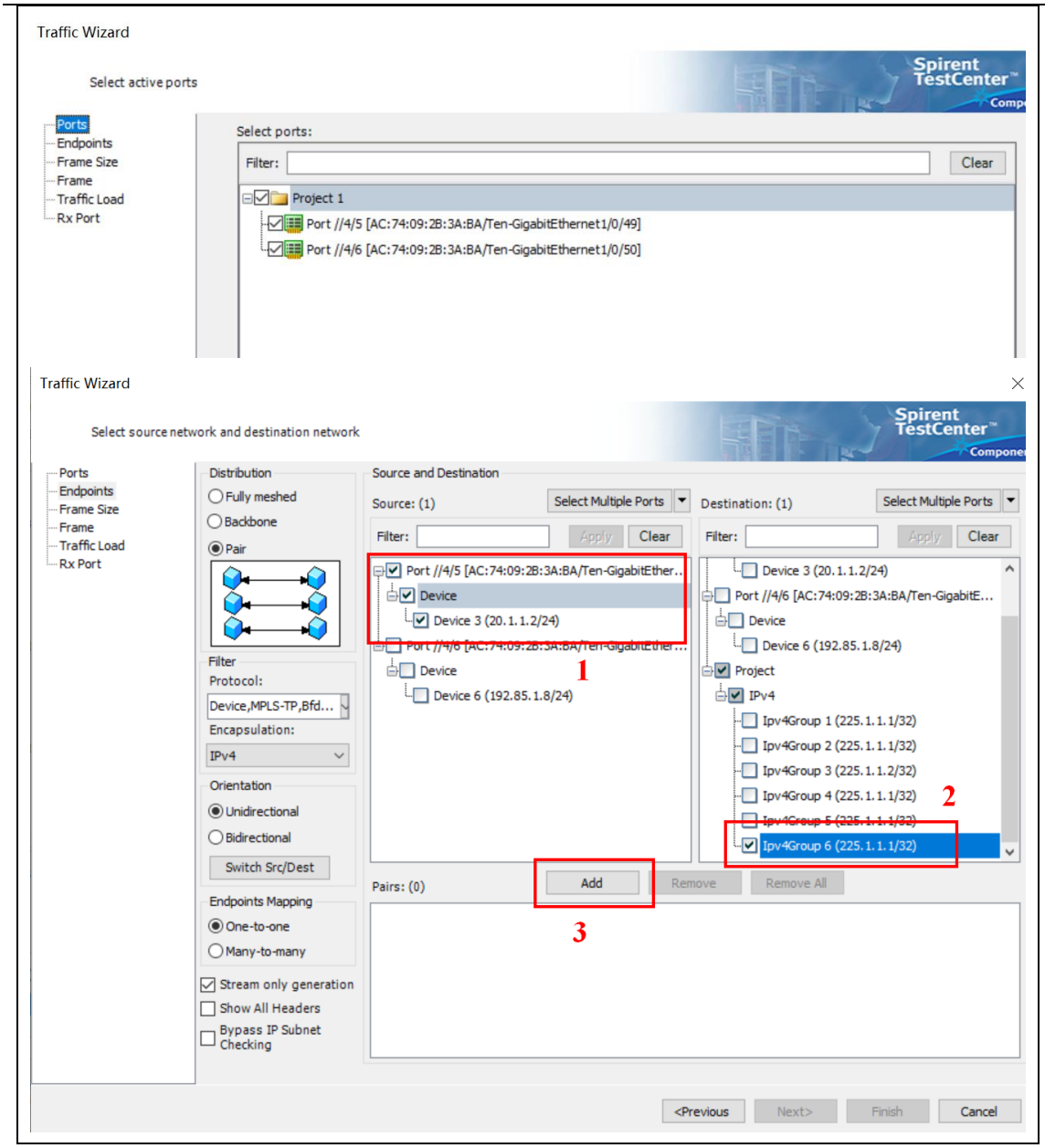


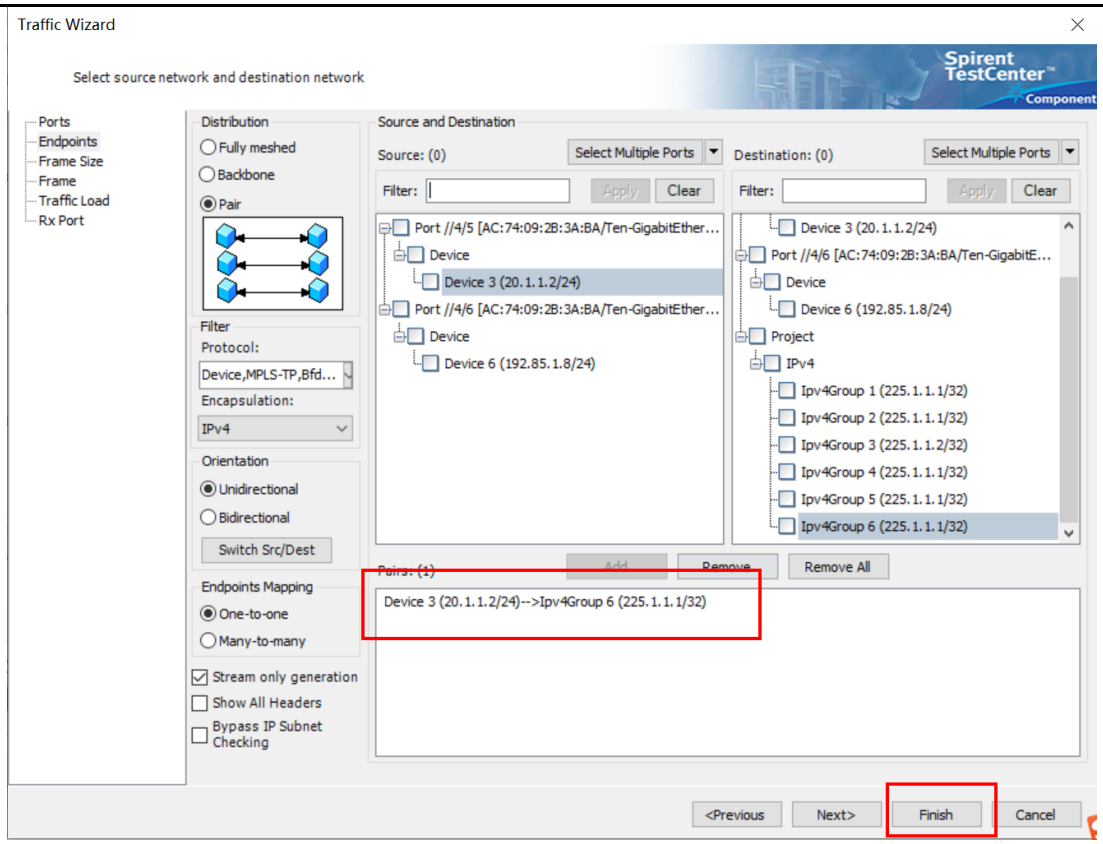
Configure multicast traffic on the multicast sending port;

Add bound stream block

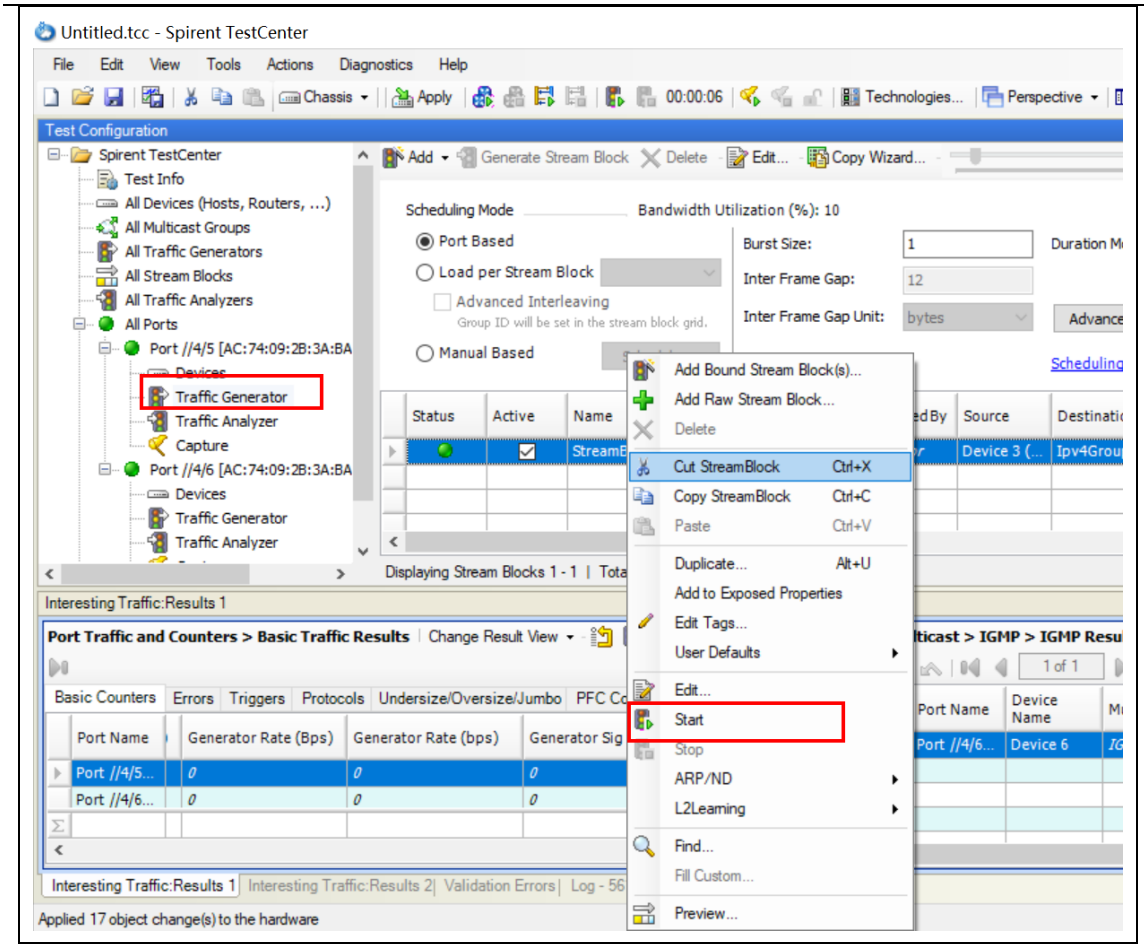


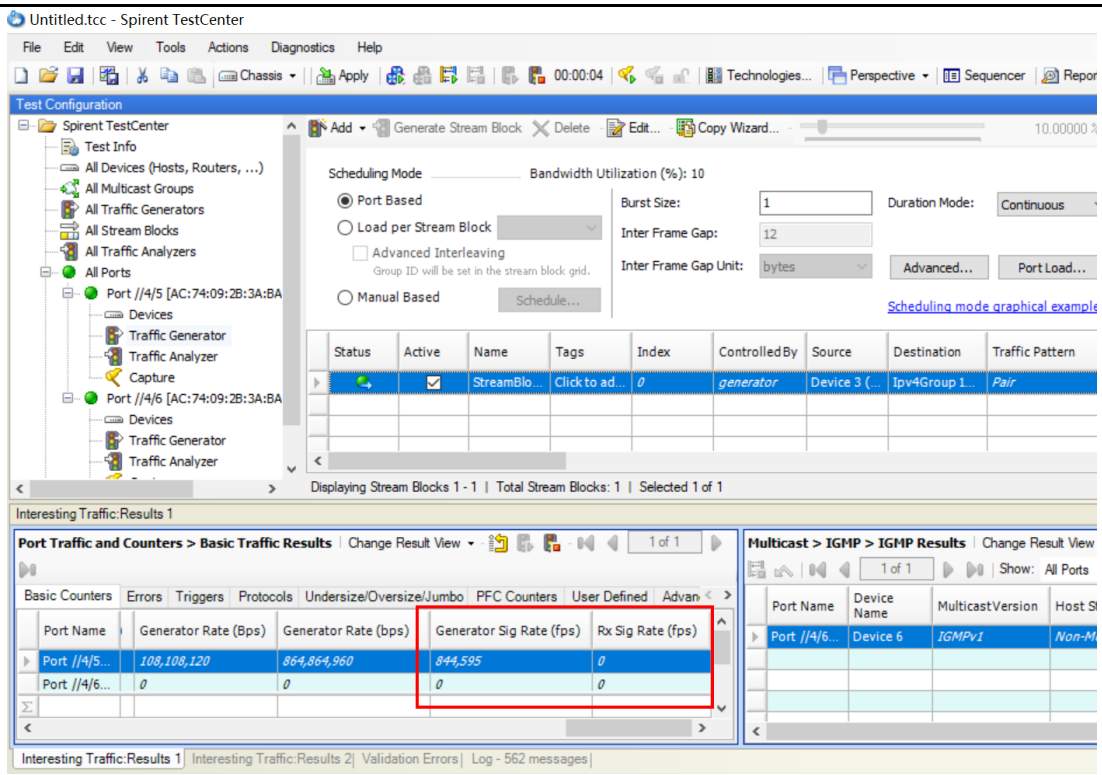
Select active port





Send the packets on Port A.

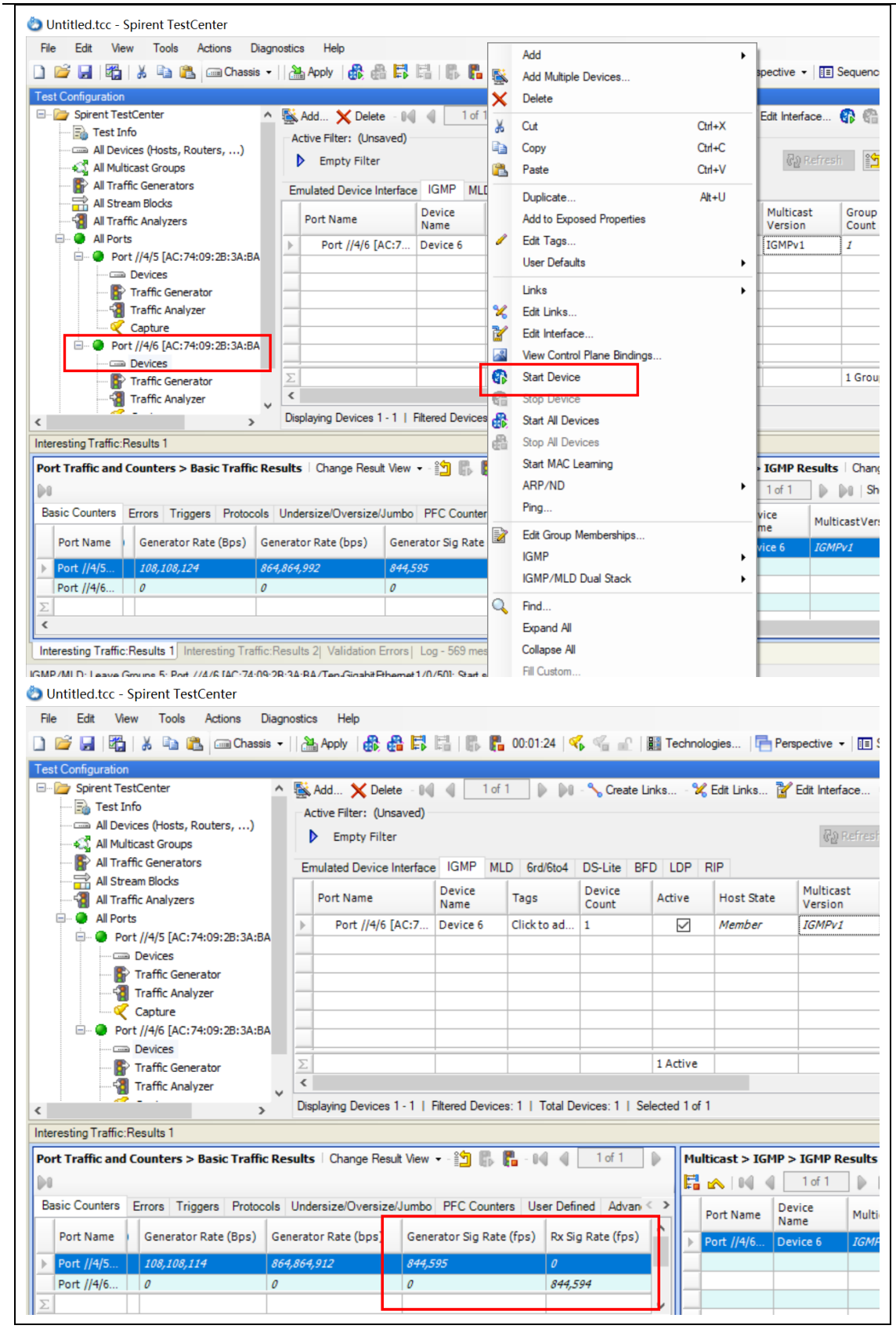

Untitled.tcc - Spirent TestCenter
File Edit View Tools Actions Diagnostics Help
Chassis Apply 00:00:06 Technologies... Perspective
Test Configuration
Spirent TestCenter
Test Info
All Devices (Hosts, Routers, ...)
All Multicast Groups
All Traffic Generators
All Stream Blocks
All Traffic Analyzers
All Ports
Port //4/5 [AC:74:09:2B:3A:BA
Devices
Traffic Generator
Traffic Analyzer
Capture
Port //4/6 [AC:74:09:2B:3A:BA
Devices
Traffic Generator
Traffic Analyzer
Add Generate Stream Block Delete Edit... Copy Wizard...
Scheduling Mode
Bandwidth Utilization (%): 10
Port Based
Load per Stream Block
Advanced Interleaving
Group ID will be set in the stream block grid.
Manual Based
Burst Size: 1
Inter Frame Gap: 12
Inter Frame Gap Unit: bytes
Status Active Name Source Destinati
Displaying Stream Blocks 1 - 1
Add Bound Stream Block(s)...
Add Raw Stream Block...
Delete
Cut StreamBlock Ctrl+X
Copy StreamBlock Ctrl+C
Paste Ctrl+V
Duplicate... Alt+U
Add to Exposed Properties
Edit Tags...
User Defaults
Edit...
Start
Stop
ARP/ND
L2Learning
Find...
Fill Custom...
Preview...
Interesting Traffic:Results 1
Port Traffic and Counters > Basic Traffic Results
Change Result View
Basic Counters Errors Triggers Protocols Undersize/Oversize/Jumbo
Port Name Generator Rate (Bps) Generator Rate (bps)
Port //4/5...
Port //4/6...
Interesting Traffic:Results 1 Interesting Traffic:Results 2 Validation Errors
Applied 17 object change(s) to the hardware



Port B doesn't receive multicast traffic.

5. Send an IGMP message from Port B of Tester to simulate joining multicast group 225.0.0.1. Result 2 is expected.

Start the device created on Port B to send the IGMP message to simulate joining multicast group 225.0.0.1


Untitled.tcc - Spirent TestCenter
File Edit View Tools Actions Diagnostics Help
Test Configuration
Spirent TestCenter
Test Info
All Devices (Hosts, Routers, ...)
All Multicast Groups
All Traffic Generators
All Stream Blocks
All Traffic Analyzers
All Ports
Port //4/5 [AC:74:09:2B:3A:BA
Devices
Traffic Generator
Traffic Analyzer
Capture
Port //4/6 [AC:74:09:2B:3A:BA
Devices
Traffic Generator
Traffic Analyzer
Add...
Delete
Active Filter: (Unsaved)
Empty Filter
Emulated Device Interface
IGMP
Port Name
Device Name
Port //4/6 [AC:7...
Device 6
Displaying Devices 1 - 1 | Filtered Devices
Add
Add Multiple Devices...
Delete
Cut Ctrl+X
Copy Ctrl+C
Paste Ctrl+V
Duplicate... Alt+U
Add to Exposed Properties
Edit Tags...
User Defaults
Links
Edit Links...
Edit Interface...
View Control Plane Bindings...
Start Device
Stop Device
Start All Devices
Stop All Devices
Start MAC Learning
ARP/ND
Ping...
Edit Group Memberships...
IGMP
IGMP/MLD Dual Stack
Find...
Expand All
Collapse All
Fill Custom...
Edit Interface...
Refresh
Multicast Version
Group Count
IGMPv1
Interesting Traffic:Results 1
Port Traffic and Counters > Basic Traffic Results
Change Result View
Basic Counters
Errors
Triggers
Protocols
Undersize/Oversize/Jumbo
PFC Counter
Generator Rate (Bps)
Generator Rate (bps)
Generator Sig Rate
Port //4/5...
108,108,124
864,864,992
844,595
Port //4/6...
0
0
0
Interesting Traffic:Results 1
Interesting Traffic:Results 2
Validation Errors
Log - 569 mes
IGMP Results
Untitled.tcc - Spirent TestCenter
File Edit View Tools Actions Diagnostics Help
00:01:24
Technologies...
Perspective
Test Configuration
Spirent TestCenter
Test Info
All Devices (Hosts, Routers, ...)
All Multicast Groups
All Traffic Generators
All Stream Blocks
All Traffic Analyzers
All Ports
Port //4/5 [AC:74:09:2B:3A:BA
Devices
Traffic Generator
Traffic Analyzer
Capture
Port //4/6 [AC:74:09:2B:3A:BA
Devices
Traffic Generator
Traffic Analyzer
Add...
Delete
1 of 1
Create Links...
Edit Links...
Edit Interface...
Active Filter: (Unsaved)
Empty Filter
Emulated Device Interface
IGMP
MLD
6rd/6to4
DS-Lite
BFD
LDP
RIP
Port Name
Device Name
Tags
Device Count
Active
Host State
Multicast Version
Port //4/6 [AC:7...
Device 6
Click to ad...
1
Member
IGMPv1
1 Active
Displaying Devices 1 - 1 | Filtered Devices: 1 | Total Devices: 1 | Selected 1 of 1
Interesting Traffic:Results 1
Port Traffic and Counters > Basic Traffic Results
Change Result View
1 of 1
Basic Counters
Errors
Triggers
Protocols
Undersize/Oversize/Jumbo
PFC Counters
User Defined
Generator Rate (Bps)
Generator Rate (bps)
Generator Sig Rate (fps)
Rx Sig Rate (fps)
Port //4/5...
108,108,114
864,864,912
844,595
0
Port //4/6...
0
0
0
844,594
Multicast > IGMP > IGMP Results
Port Name
Device Name
Port //4/6...
Device 6

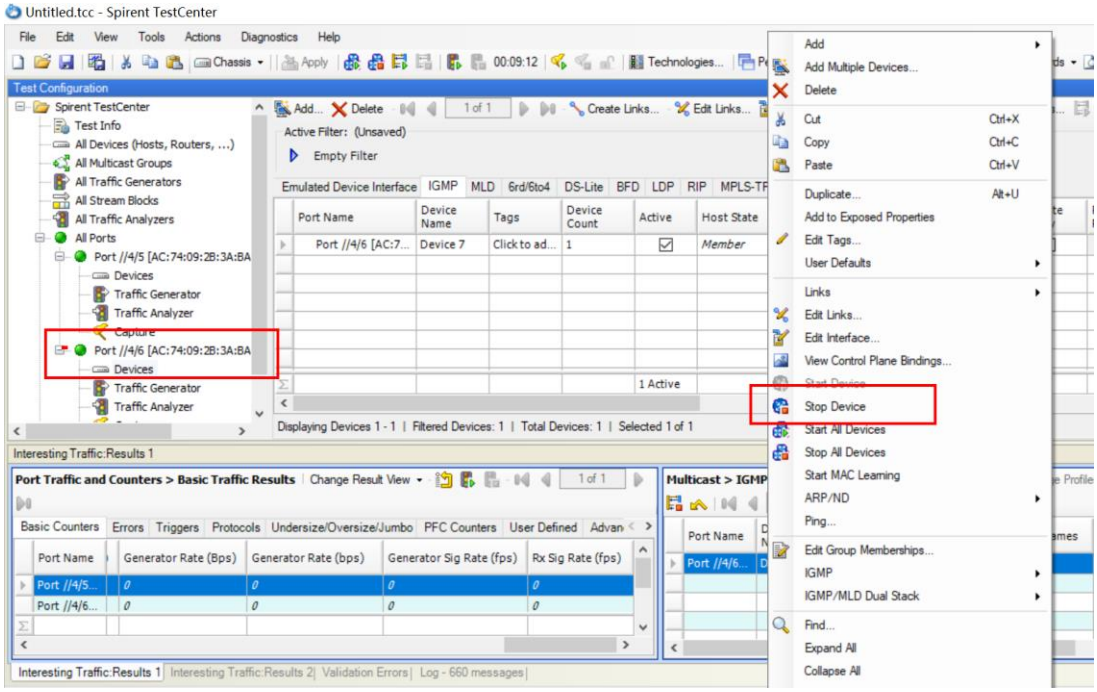
Multicast group 225.0.0.1 joined, Tester Port B receives multicast data.

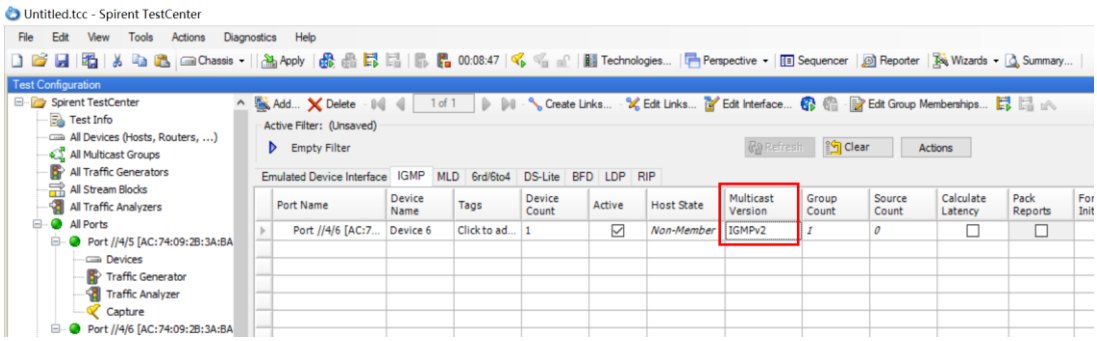
6. Enable IGMP in Vlan-interface3 interface view, set up IGMP version 2, enable pim dm in all ports:

Change the IGMP version. The default version is IGMP version 2.

```
[DUT2]interface Vlan-interface 3
[DUT2-Vlan-interface3]igmp version 2
```

Stop the device on Port 4/6. Change the IGMP protocol, change the multicast version to IGMPv2.

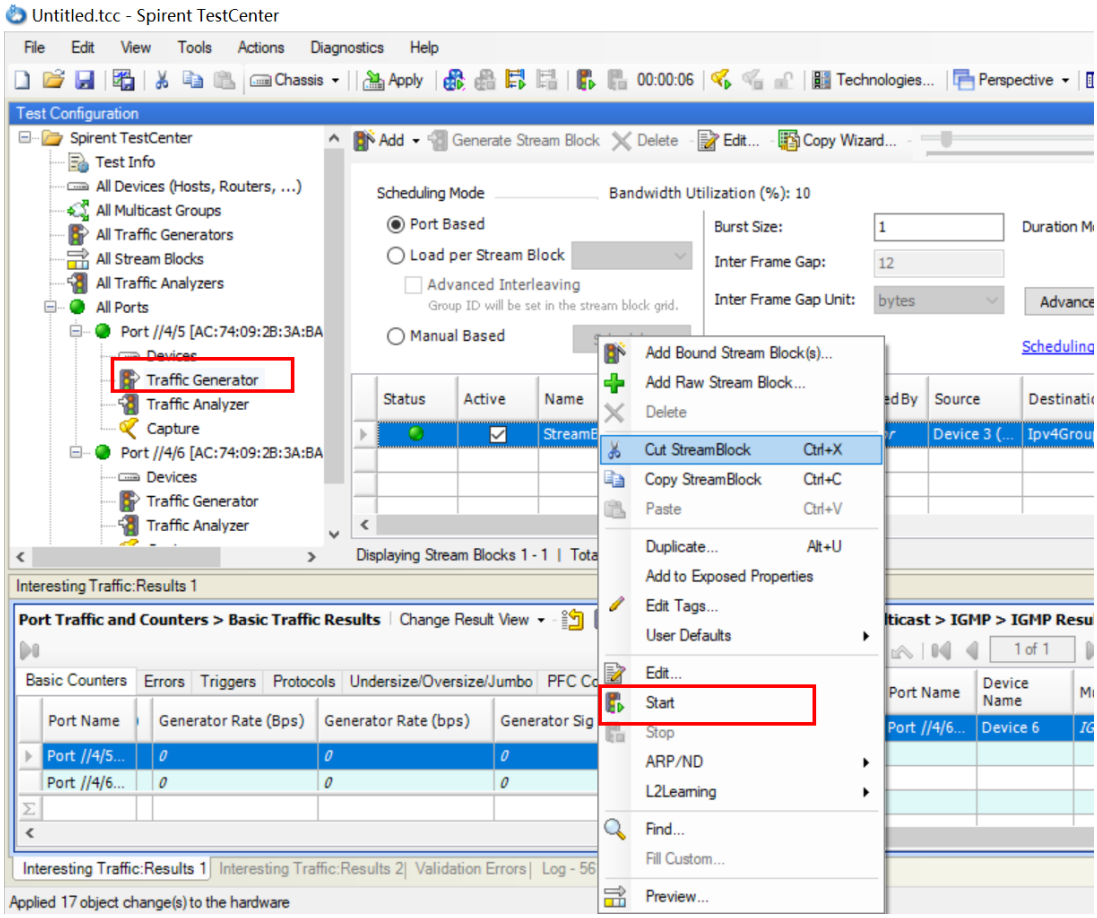




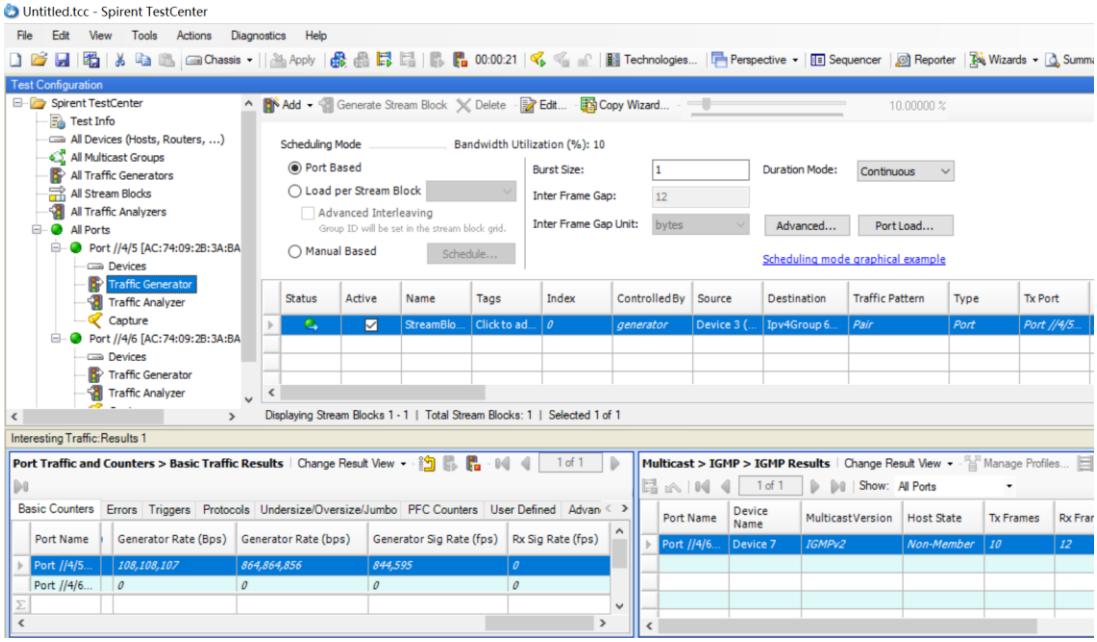
7. Send multicast data of 225.0.0.1 from Port A of Tester to DUT. Result 1 is expected.

Configure multicast traffic on the multicast sending port;

Send the packets on Port A.

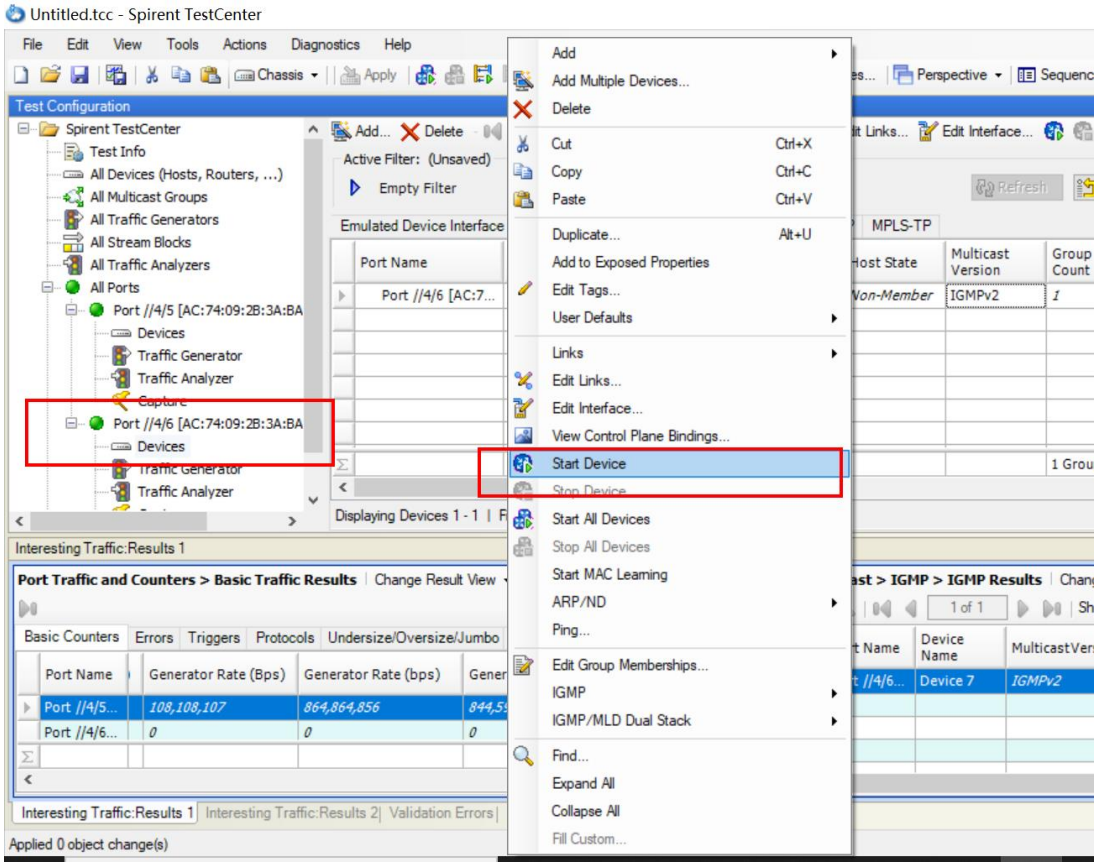


Port B doesn't receive multicast traffic.

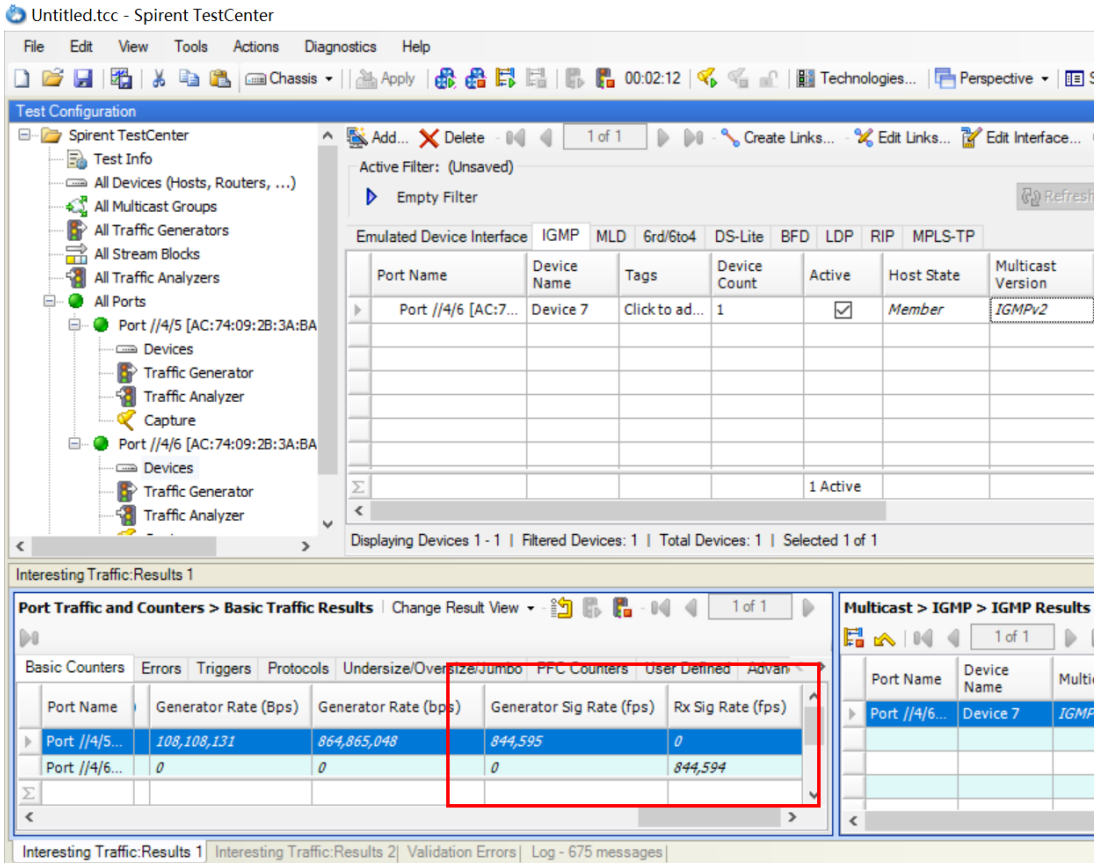


8. Send an IGMP message from Port B of Tester to simulate joining multicast group 225.0.0.1. Result 2 is expected.

Start the device created on Port B to send the IGMP message to simulate joining multicast group 225.0.0.1

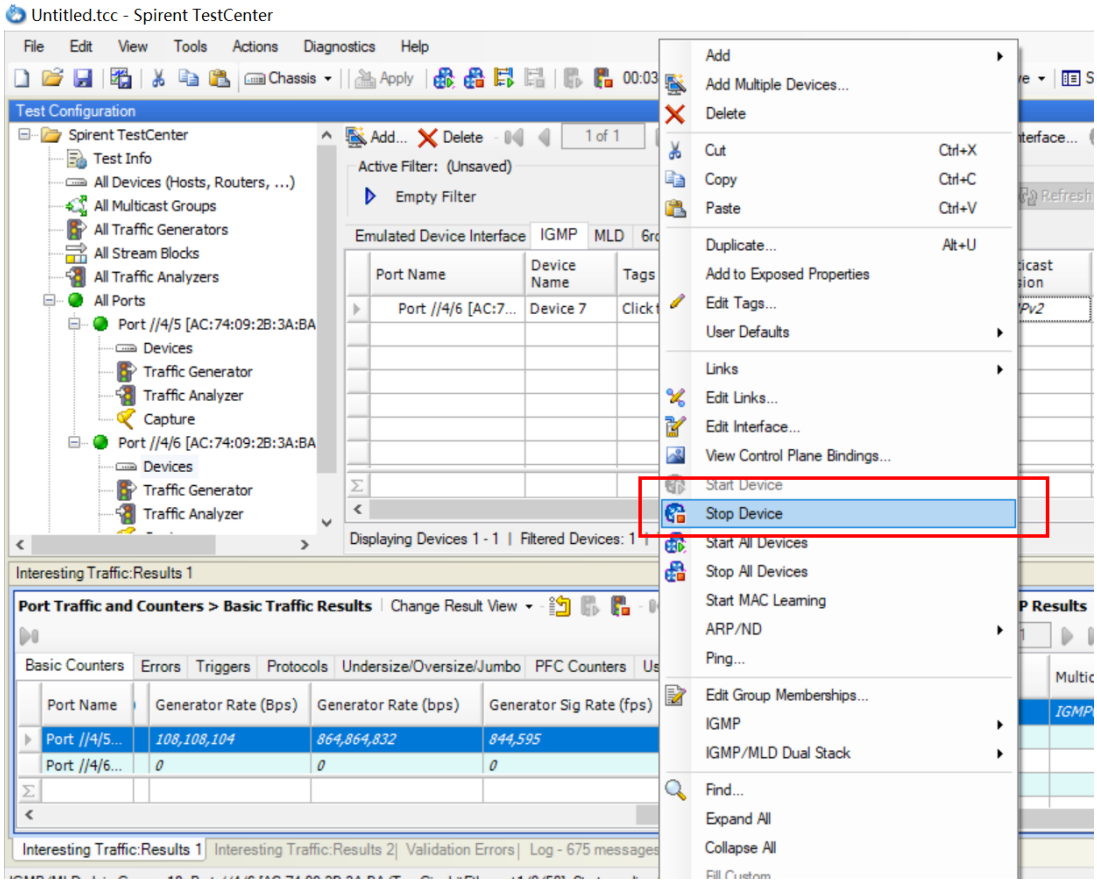


Multicast group 225.0.0.1 joined, Tester Port B receives multicast data.

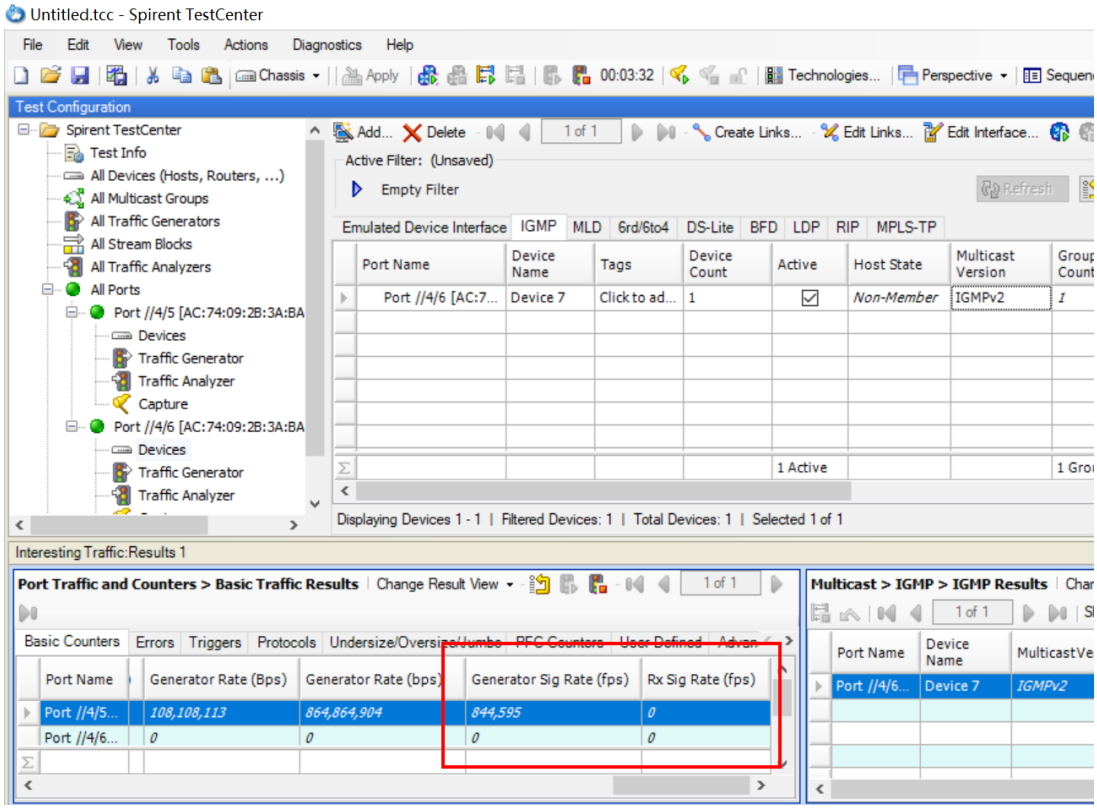


9. Send an IGMP message from Port B of Tester to simulate leaving multicast group 225.0.0.1. Result 1 is expected.

Stop the device on Port 4/6 to simulate leaving multicast group 225.0.0.1.



Multicast group 225.0.0.1 leaved, Tester Port B doesn't receive multicast data.

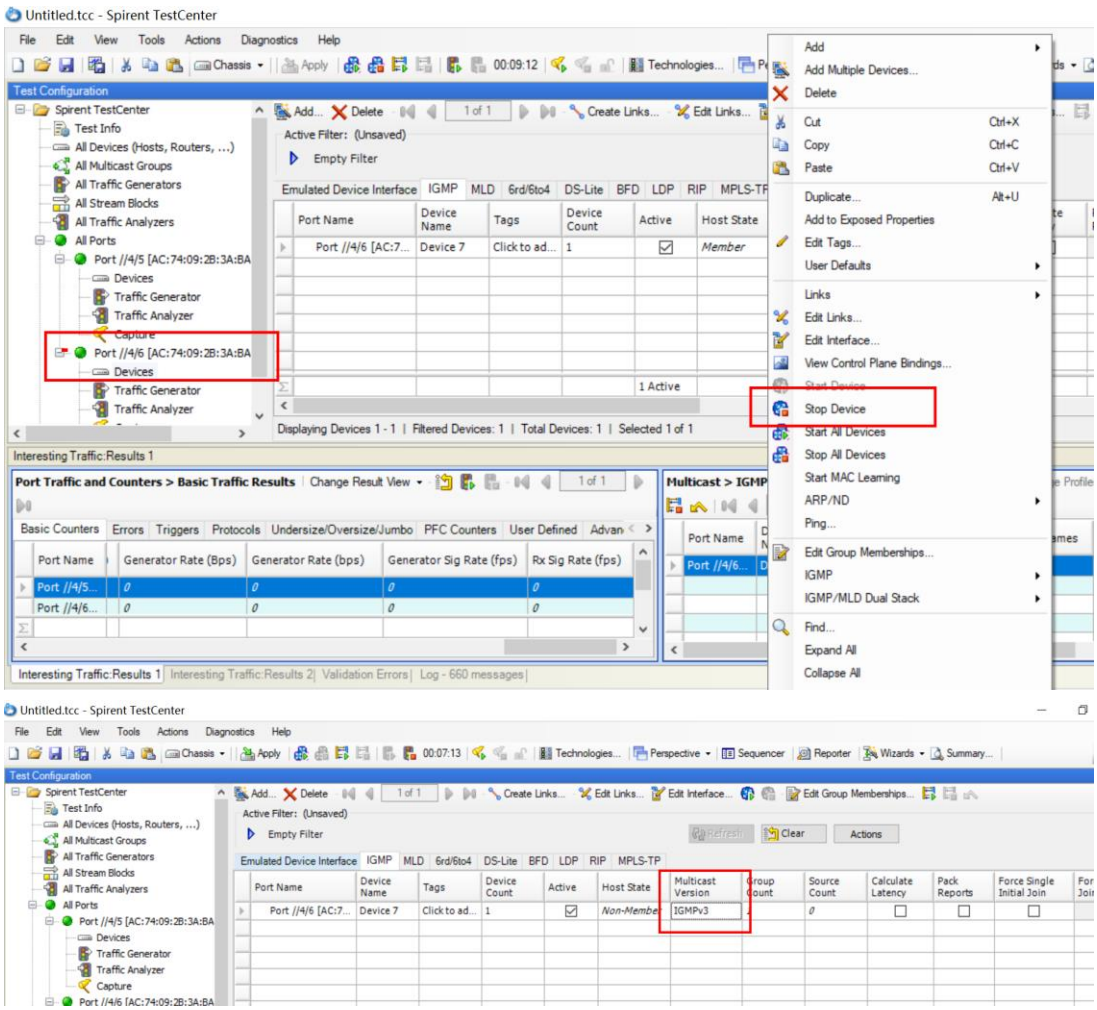


10. Enable IGMP in Vlan-interface3 interface view, set up IGMP version 3, enable PIM DM in all layer 3 ports:

Change the IGMP version. The default version is IGMP version 3.

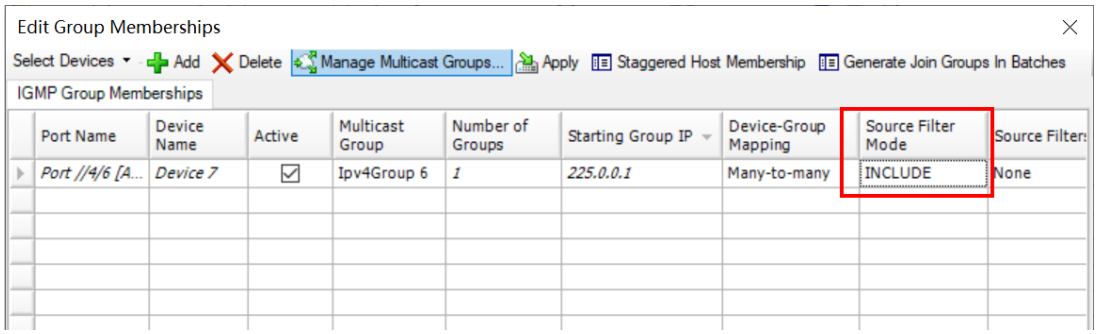
```
[DUT2]interface Vlan-interface 3
[DUT2-Vlan-interface3]igmp version 3
```

Stop the device on Port 4/6. Change the IGMP protocol, change the multicast version to IGMPv3.

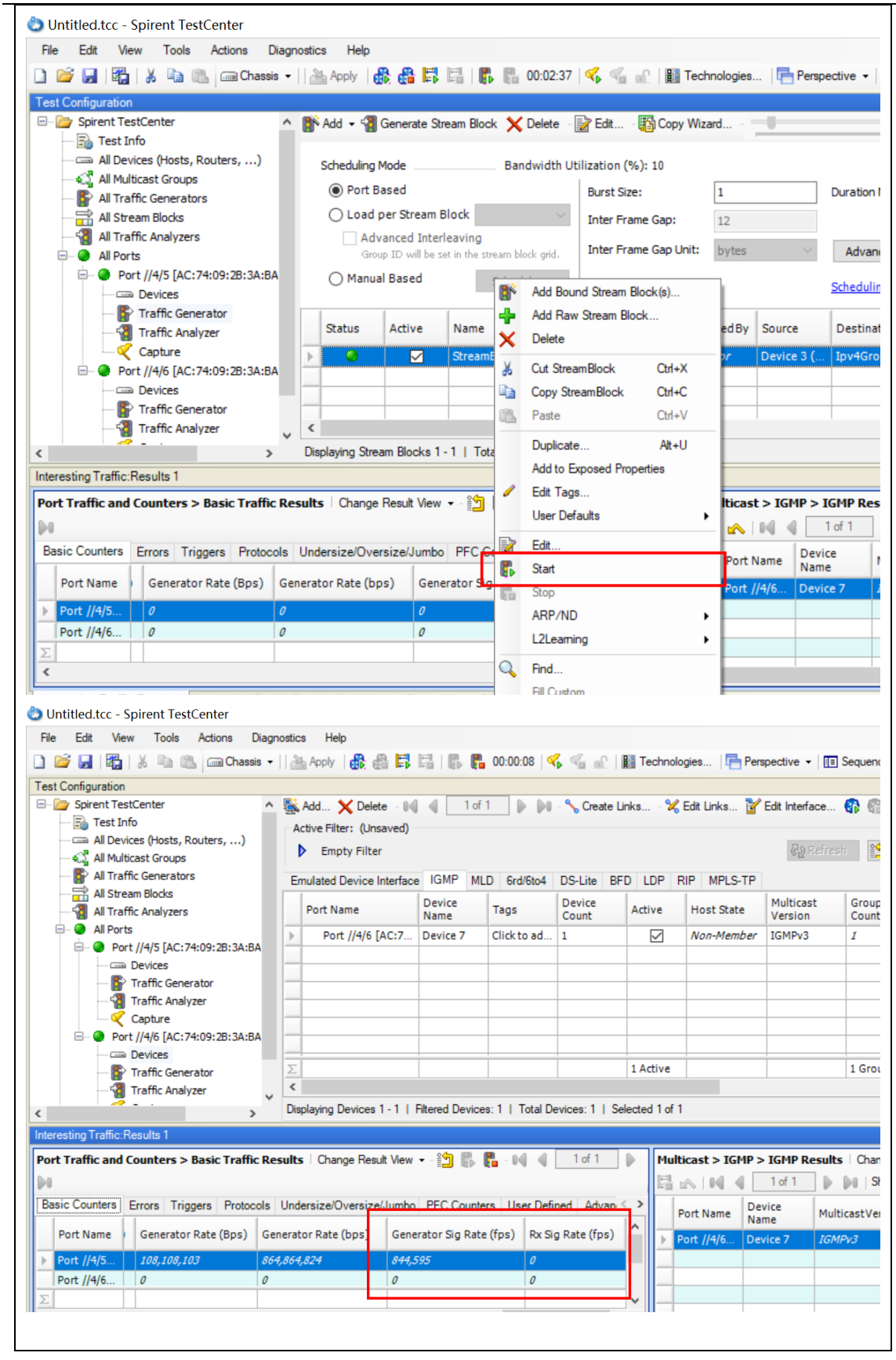


11. Send multicast data of 225.0.0.1 from Port A of Tester to DUT, source address is the port A address of Tester. Result 1 is expected.

Edit multicast group members. Change the sourec filter mode to INCLUDE.

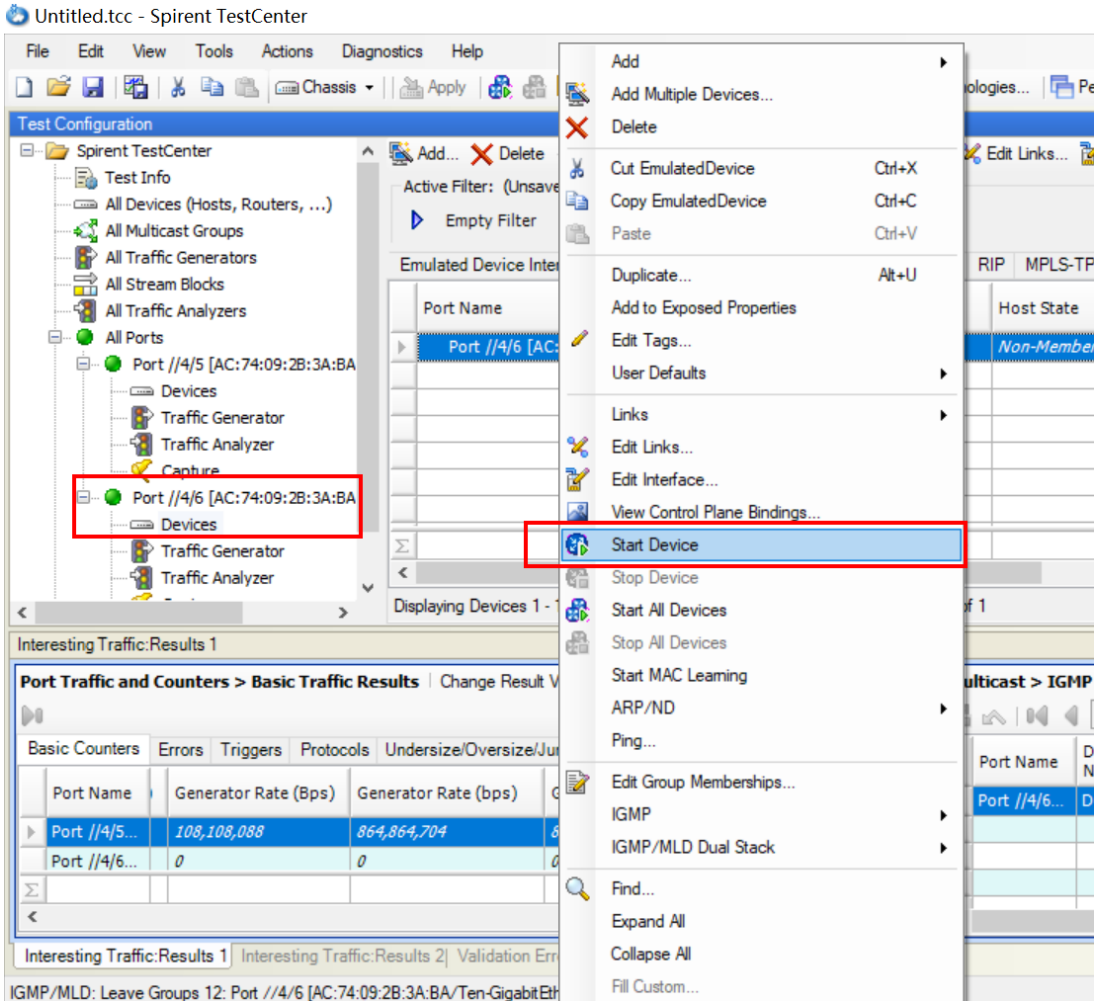


Use Port 4/5 to send multicast packets.

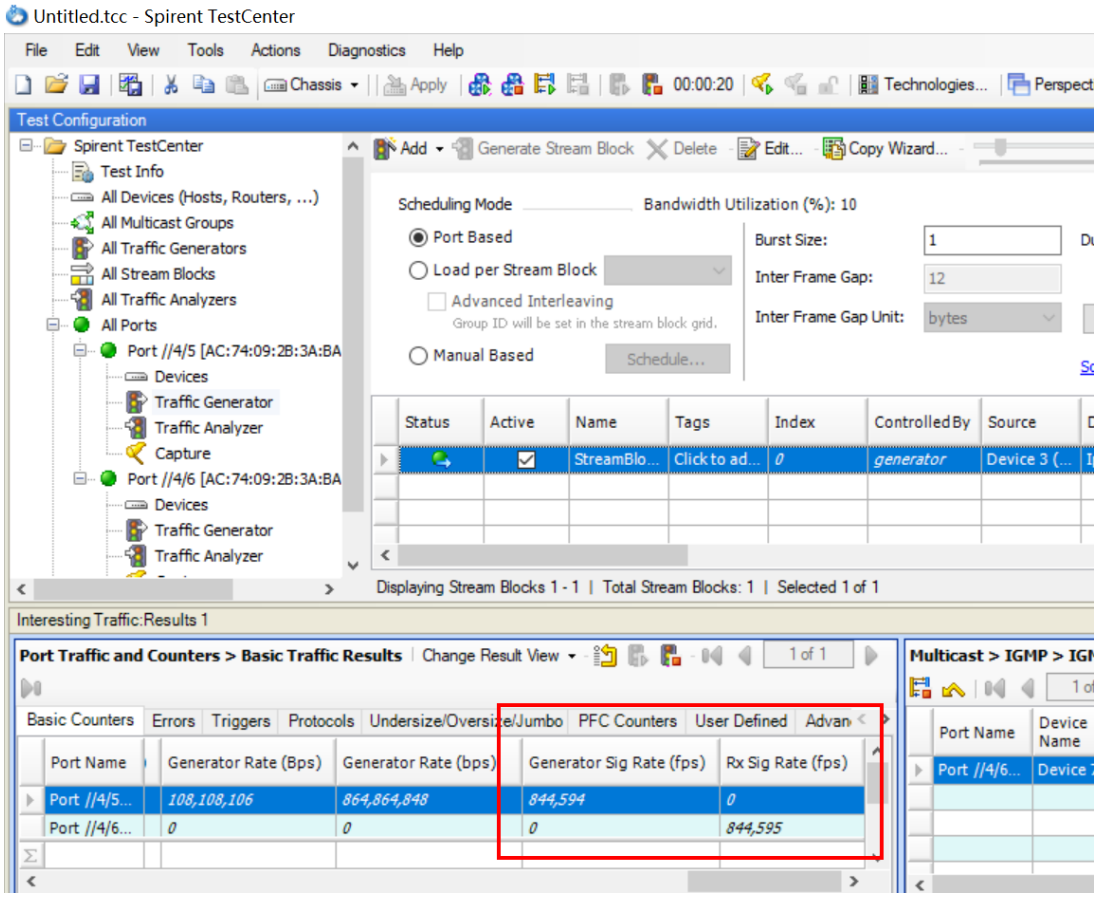


12. Send an IGMPv3 message from Port B of Tester to simulate joining multicast group IS_IN (A) of 225.0.0.1, A indicates the port A address of Tester. Result 3 is expected.

Start the device created on Port B to send the IGMP message to simulate joining multicast group IS_IN (A) of 225.0.0.1

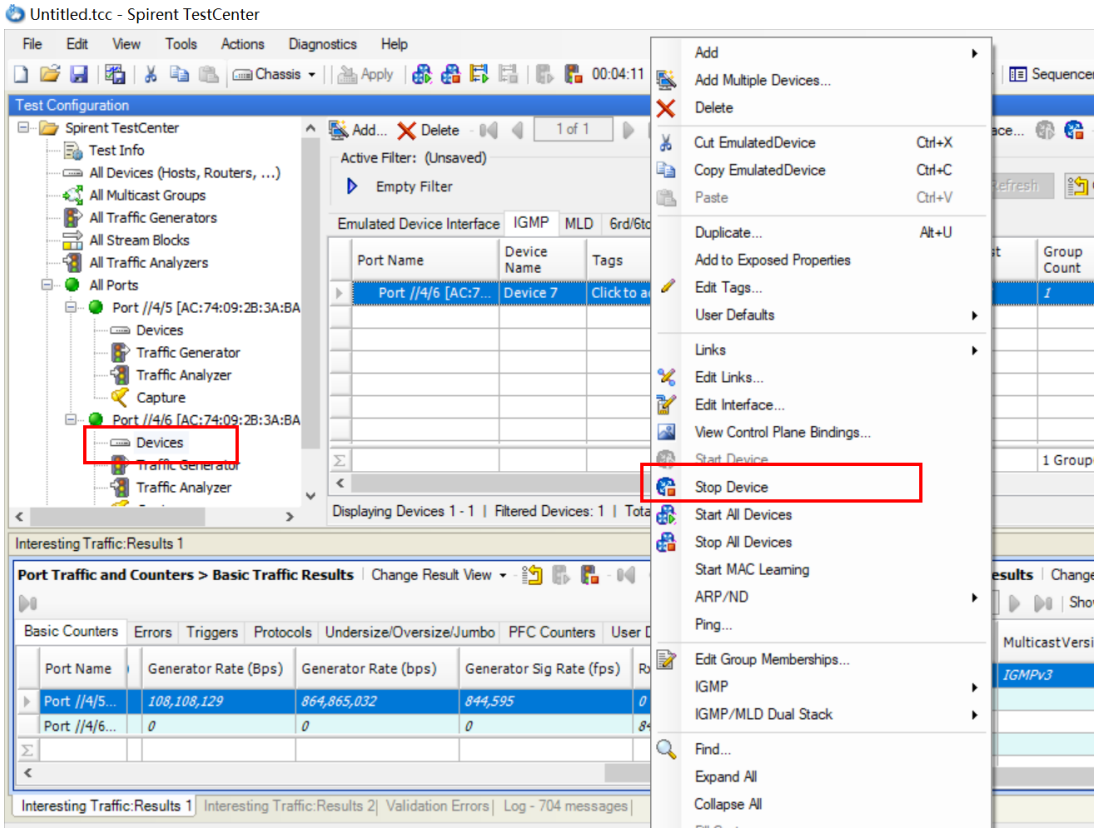


Multicast group 225.0.0.1 joined, Tester Port B receives multicast data.



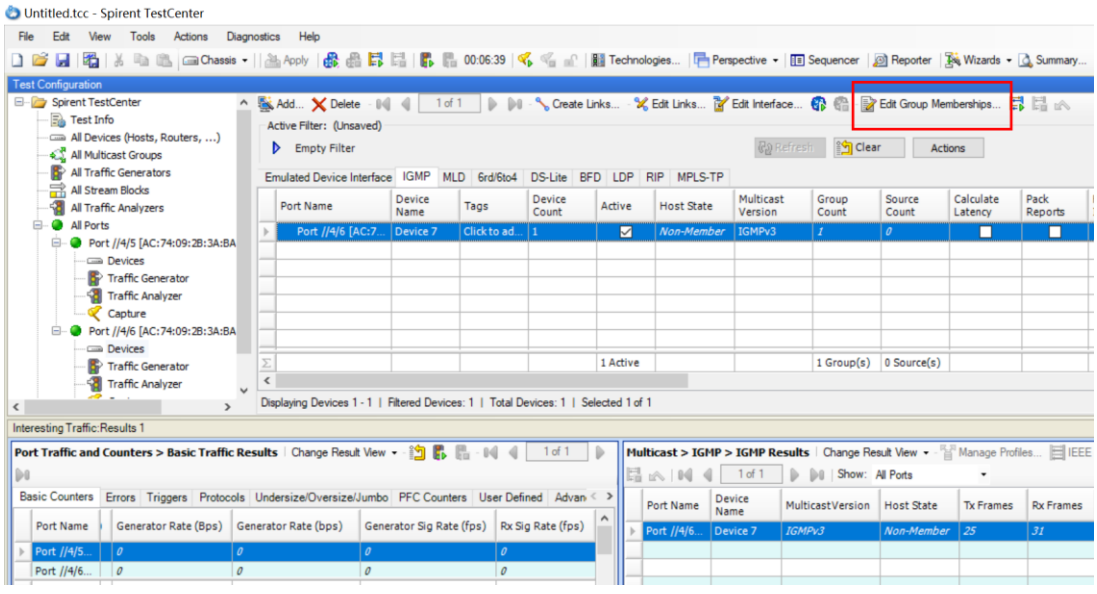
13. Tester port B leaves multicast group IS_IN（A）of 225.0.0.1. Result A is expected.

Stop the device on Port 4/6 to simulate leaving multicast group IS_IN（A）of 225.0.0.1.

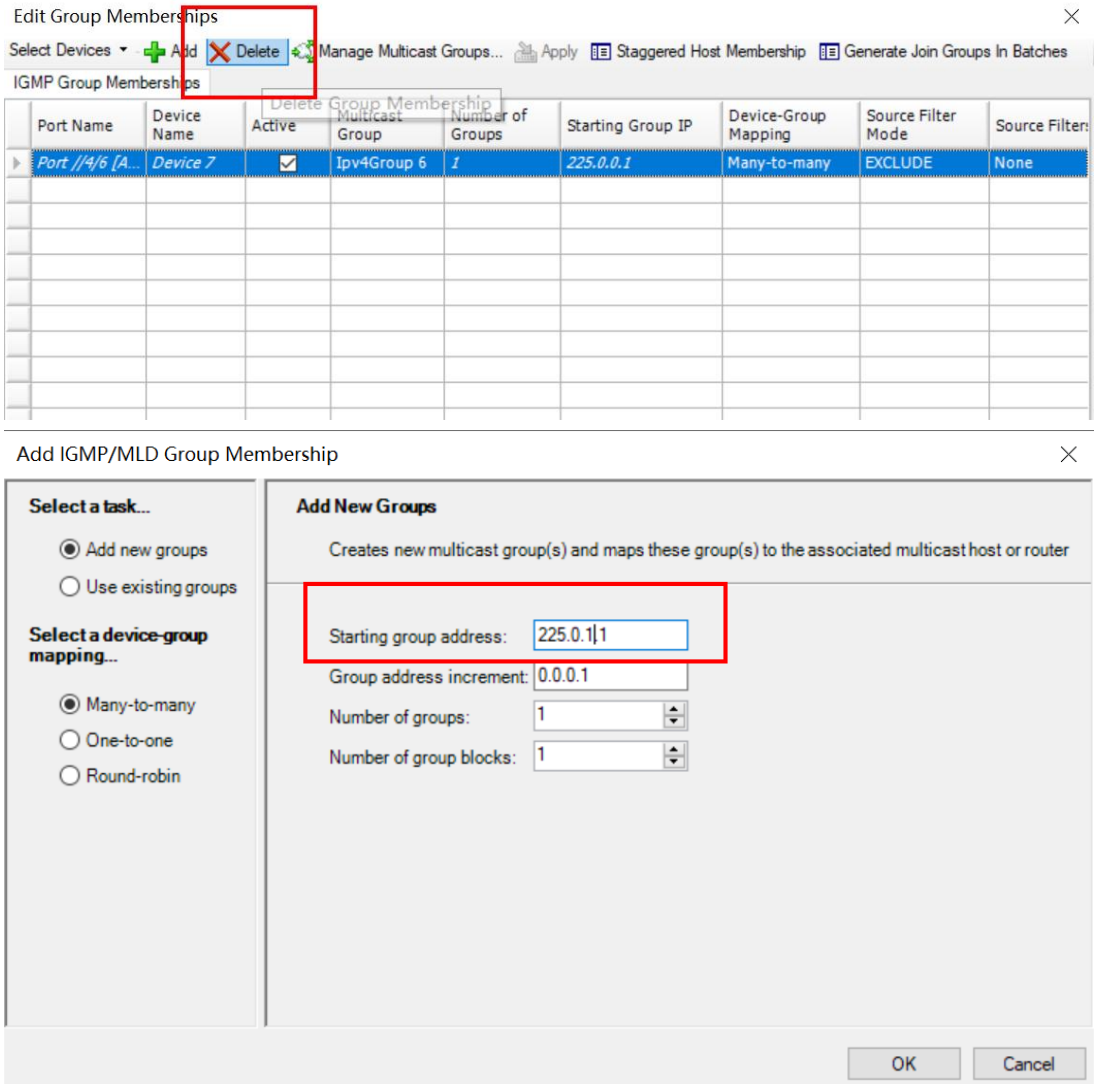


14. Send an IGMPv3 message from Port B of Tester to simulate joining multicast group IS_IN (not A) of 225.0.0.1. Result 4 is expected.

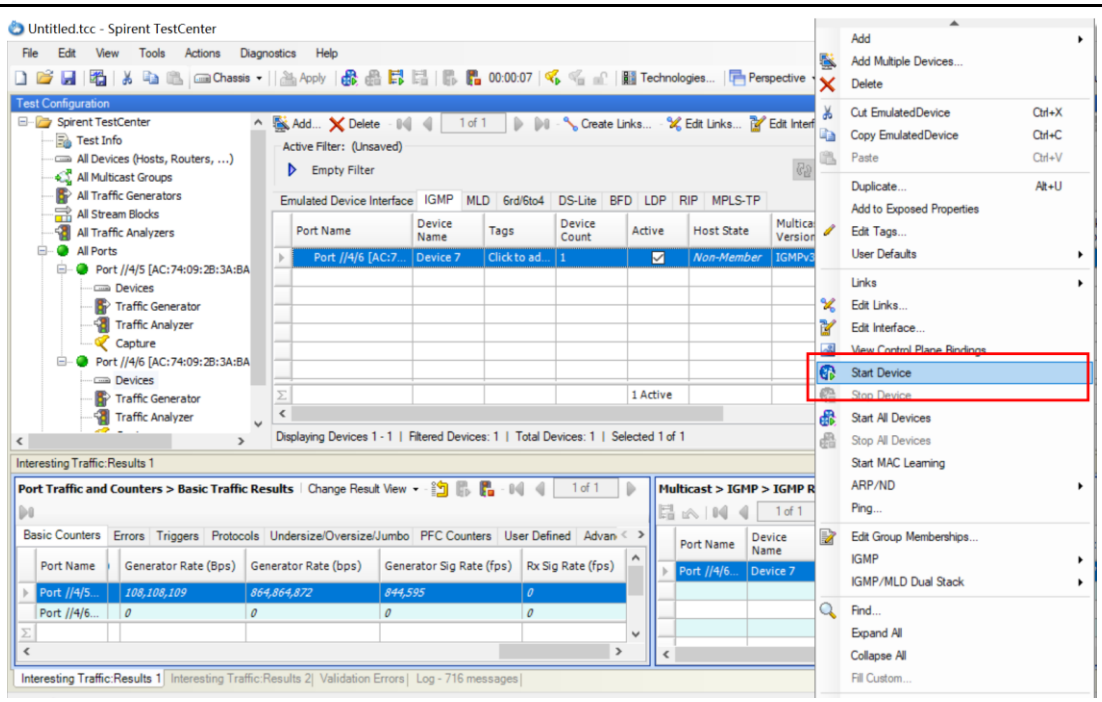
Edit the multicast group memberships.



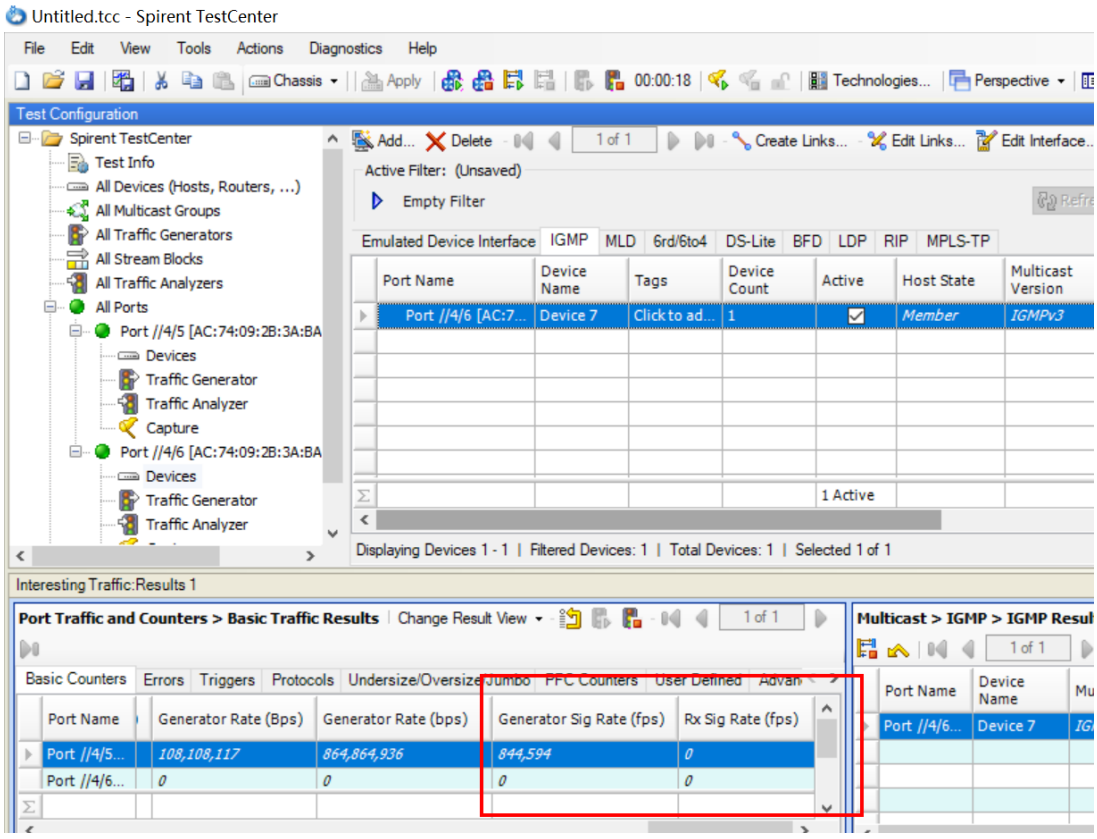
Delete the existing member, add a new member with the address which it not 225.0.0.1.



Use Port A send the multicast packets and start the device created on Port B to send the IGMP message to simulate joining multicast group IS_IN (not A).



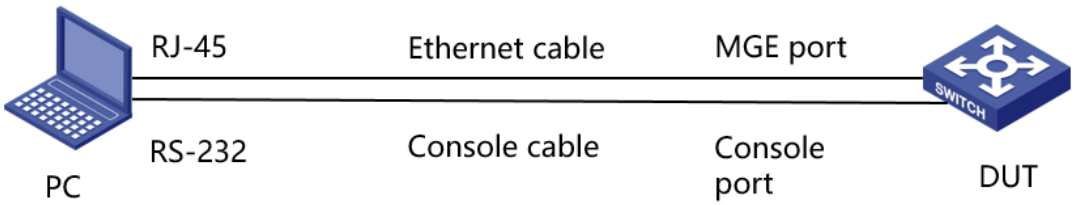
Multicast group 225.0.0.1 joined, Tester Port B doesn't receive multicast data.

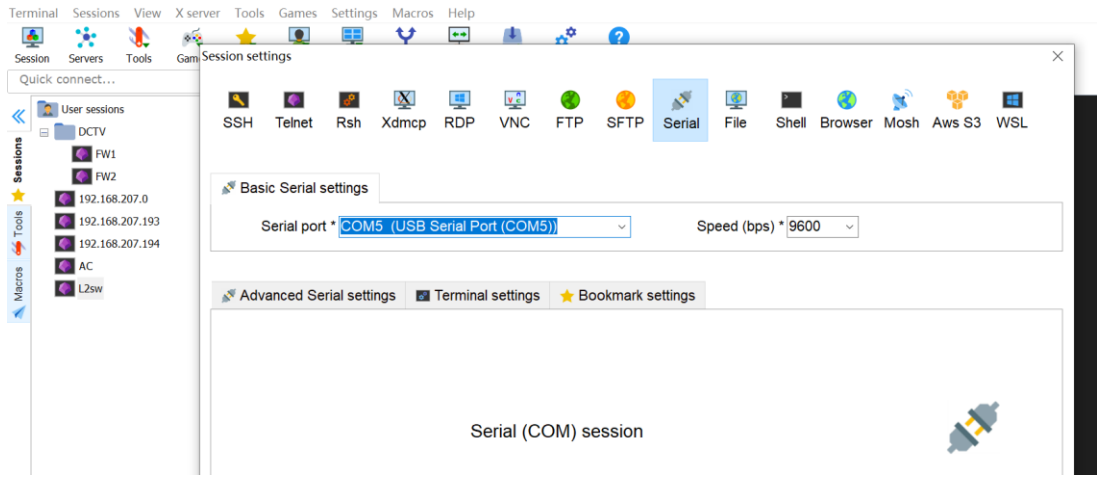


☐ Passed	☐ Failed

4 Network management

4.1 Authentication to CLI

Test Item Name: Authentication to CLI
Work Hour: 25 min
Test Topology: 
Test Process: 1. Log in to the device through the console Port. 2. Configure to enable Telnet and SSH server authentication 3. Use Telnet/SSH to connect the device with Result 1 4. Configure to enable the aux authentication 5. Use console Port to access the device with Result 1 6. Configure ACL to deny IP 192.168.207.3 and permit others 7. Configure to enable restricting access by telnet based on ACL 8. Configure the IP address 192.168.207.3 for PC 9. Use PC to access the device by telnet with Result 2 10. Configure the IP address 192.168.207.28 for PC 11. Use PC to access the device by telnet with Result 1
Expect Results: 1. You can login the device by console/Telnet/SSH with the configured account successfully and DUT allows 8 concurrent sessions by Telnet/SSH 2. Fail to connect to the device
Actual Result： 1. Log in to the device through the console Port.

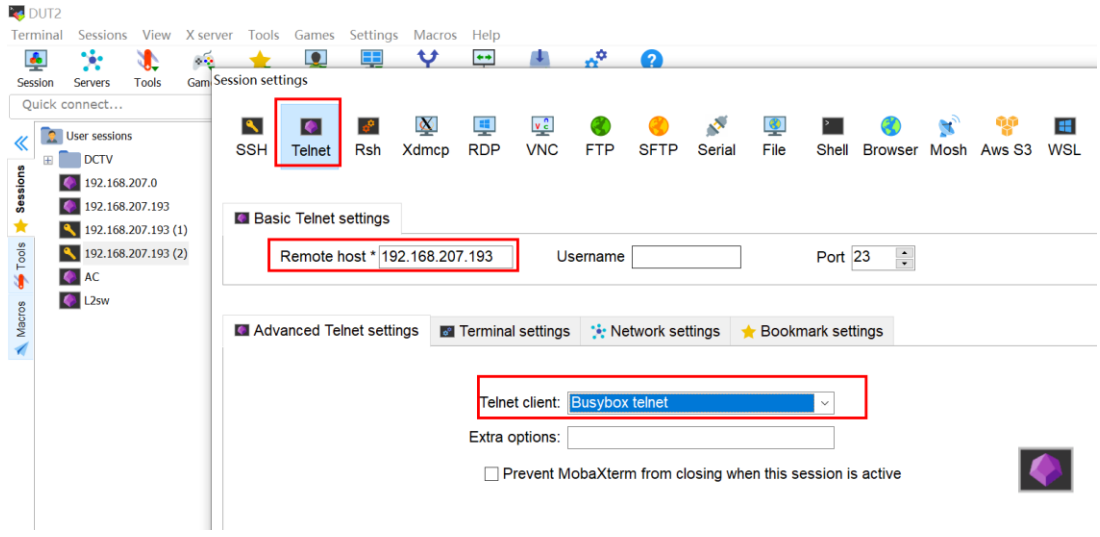


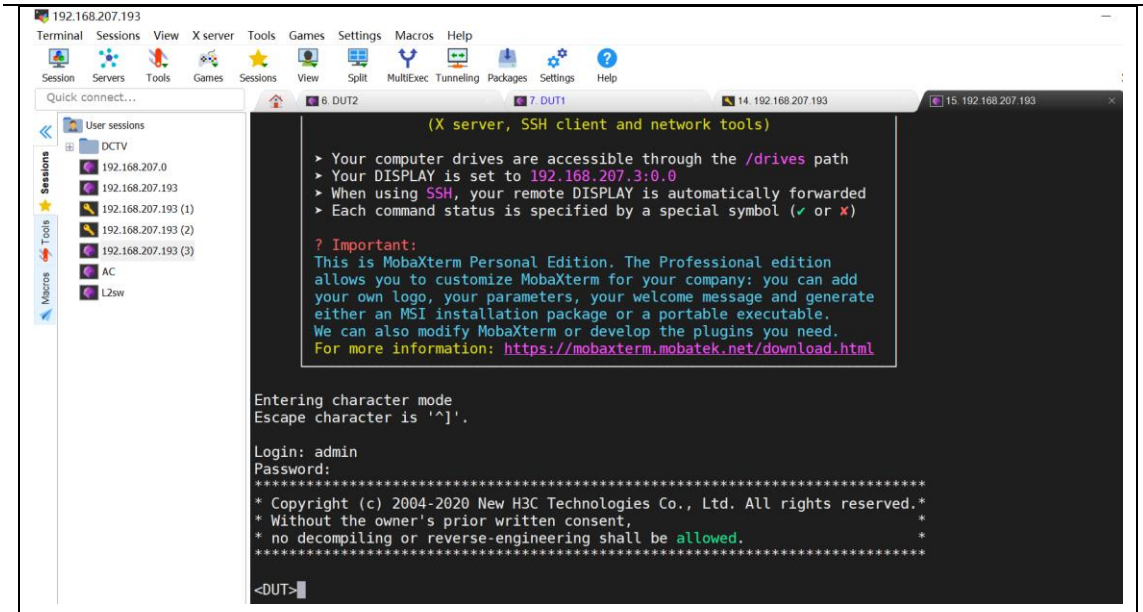
2. Configure to enable Telnet and SSH server authentication

```
[DUT]telnet server enable
[DUT]ssh server enable
[DUT]line vty 0 63
[DUT-line-vty0-63]authentication-mode scheme
[DUT-line-vty0-63]user-role network-admin
[DUT]local-user admin class manage
[DUT-luser-manage-admin]password simple 123456abcd
[DUT-luser-manage-admin]service-type telnet ssh
[DUT-luser-manage-admin]authorization-attribute user-role network-admin
```

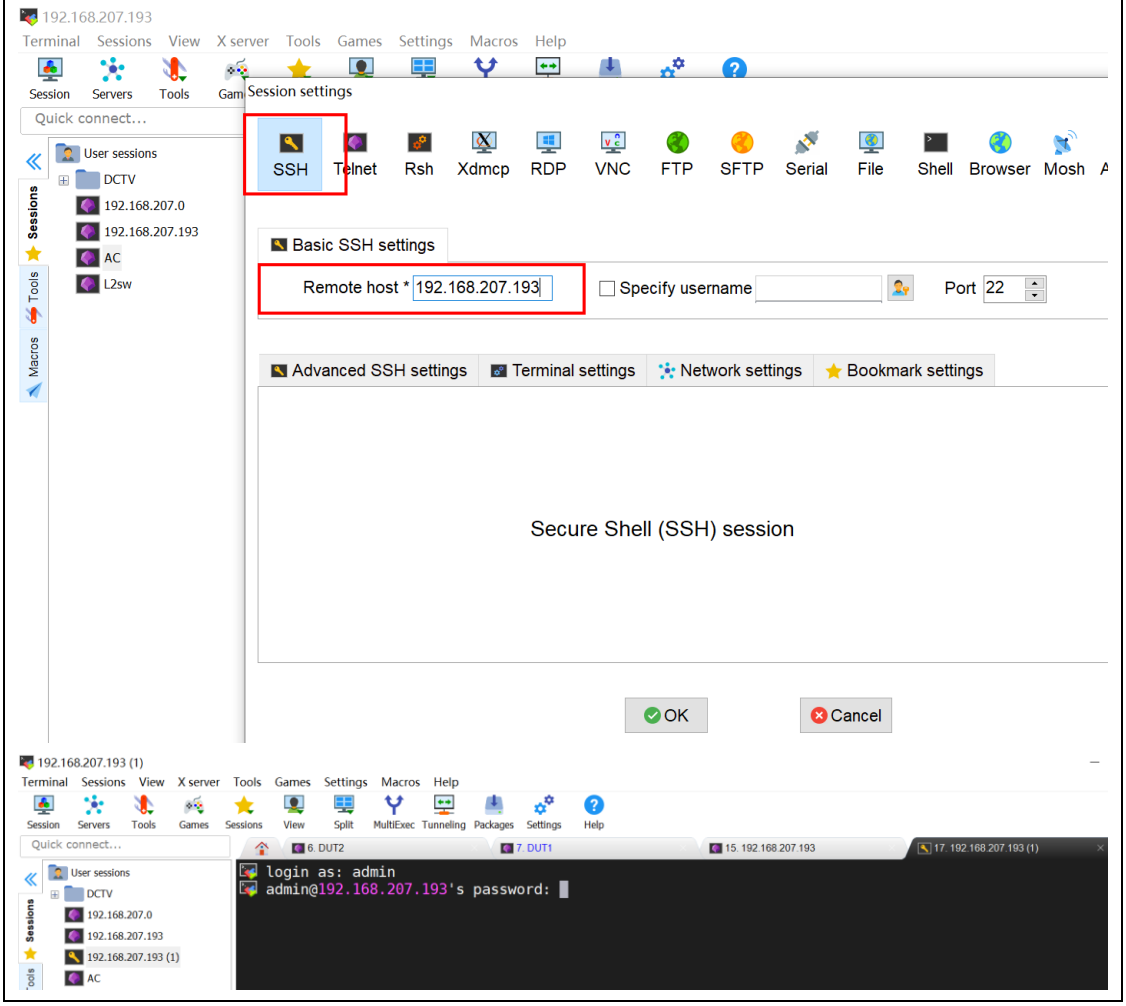
3. Use Telnet/SSH to connect the device with Result 1

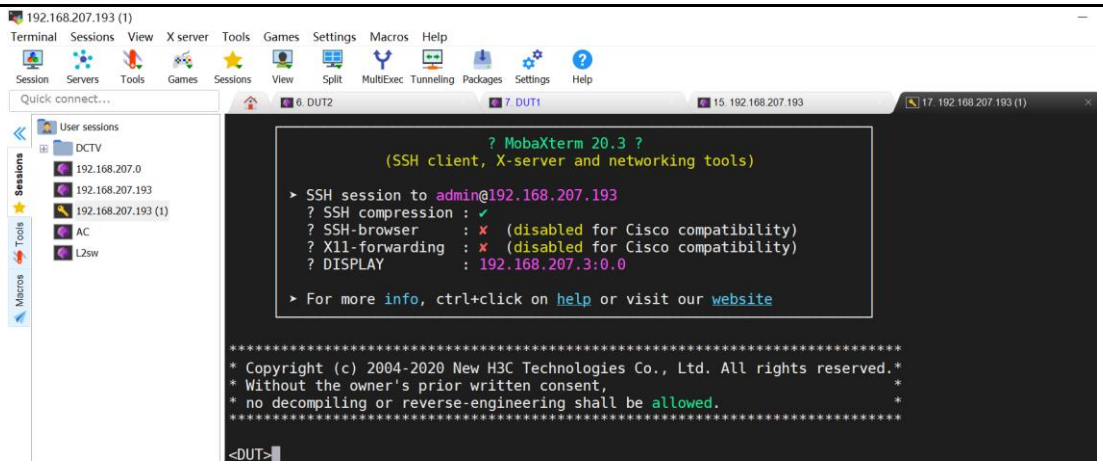
Use Telnet




192.168.207.193
Terminal Sessions View X server Tools Games Settings Macros Help
(X server, SSH client and network tools)
Your computer drives are accessible through the /drives path
Your DISPLAY is set to 192.168.207.3:0.0
When using SSH, your remote DISPLAY is automatically forwarded
Each command status is specified by a special symbol (✔ or ✘)
? Important:
This is MobaXterm Personal Edition. The Professional edition
allows you to customize MobaXterm for your company: you can add
your own logo, your parameters, your welcome message and generate
either an MSI installation package or a portable executable.
We can also modify MobaXterm or develop the plugins you need.
For more information: https://mobaxterm.mobatek.net/download.html
Entering character mode
Escape character is '^]'.
Login: admin
Password:
* Copyright (c) 2004-2020 New H3C Technologies Co., Ltd. All rights reserved.*
* Without the owner's prior written consent, *
* no decompiling or reverse-engineering shall be allowed. *
<DUT>

Use SSH:

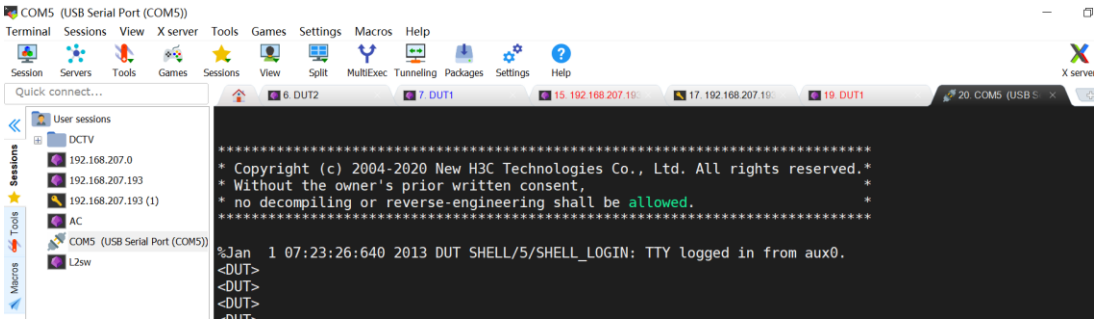

192.168.207.193
Session settings
SSH Telnet Rsh Xdmcp RDP VNC FTP SFTP Serial File Shell Browser Mosh
Basic SSH settings
Remote host * 192.168.207.193
Specify username
Port 22
Advanced SSH settings
Terminal settings
Network settings
Bookmark settings
Secure Shell (SSH) session
OK
Cancel
192.168.207.193 (1)
login as: admin
admin@192.168.207.193's password:



4. Configure to enable the aux authentication

```
[DUT]user-interface aux 0
[DUT-line-aux0]user-role network-admin
```

5. Use console Port to access the device with Result 1



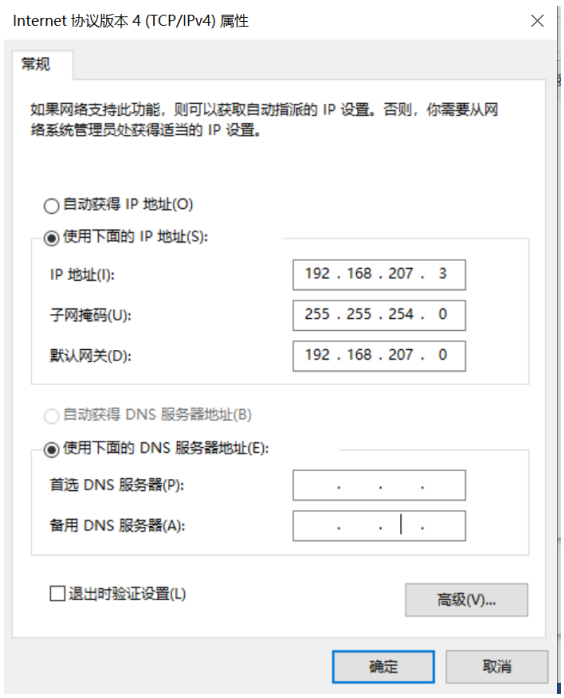
6. Configure ACL to deny IP 192.168.207.3 and permit others

```
[DUT1]acl number 2000
[DUT1-acl-ipv4-basic-2000]rule 0 deny source 192.168.207.3 0
[DUT1-acl-ipv4-basic-2000]rule 5 permit
```

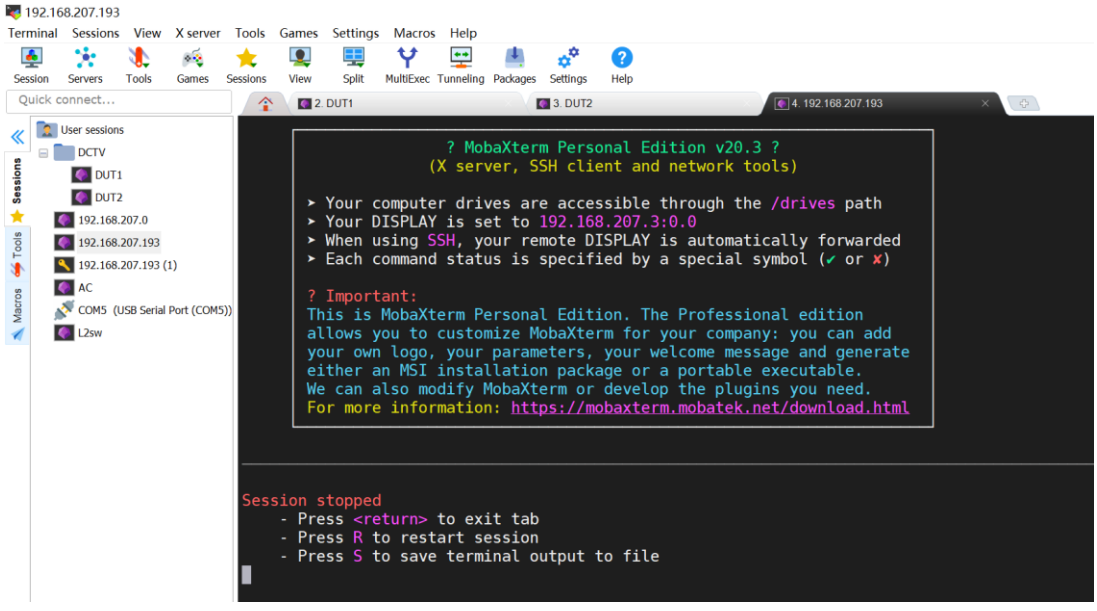
7. Configure to enable restricting access by telnet based on ACL

```
[DUT1]interface GigabitEthernet 1/0/5
[DUT1-GigabitEthernet1/0/5]packet-filter 2000 inbound
```

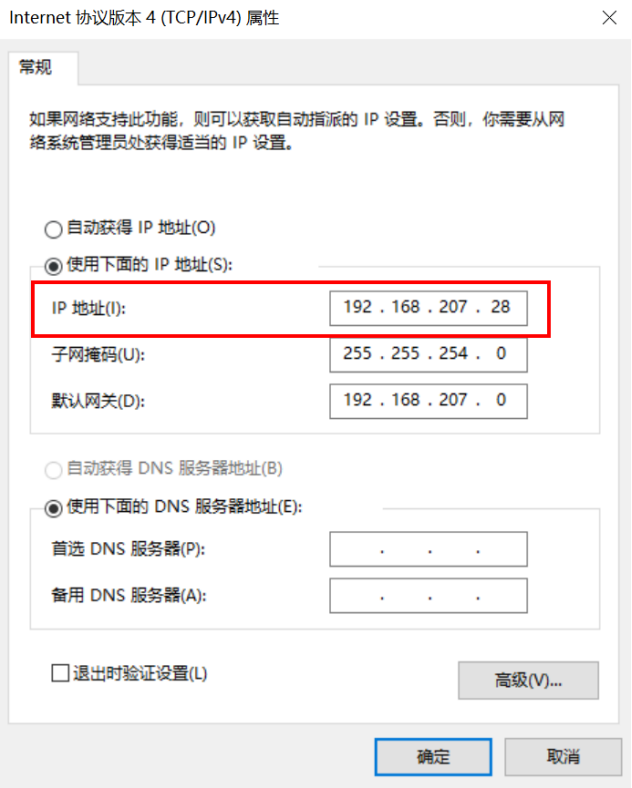
8. Configure the IP address 192.168.207.3 for PC



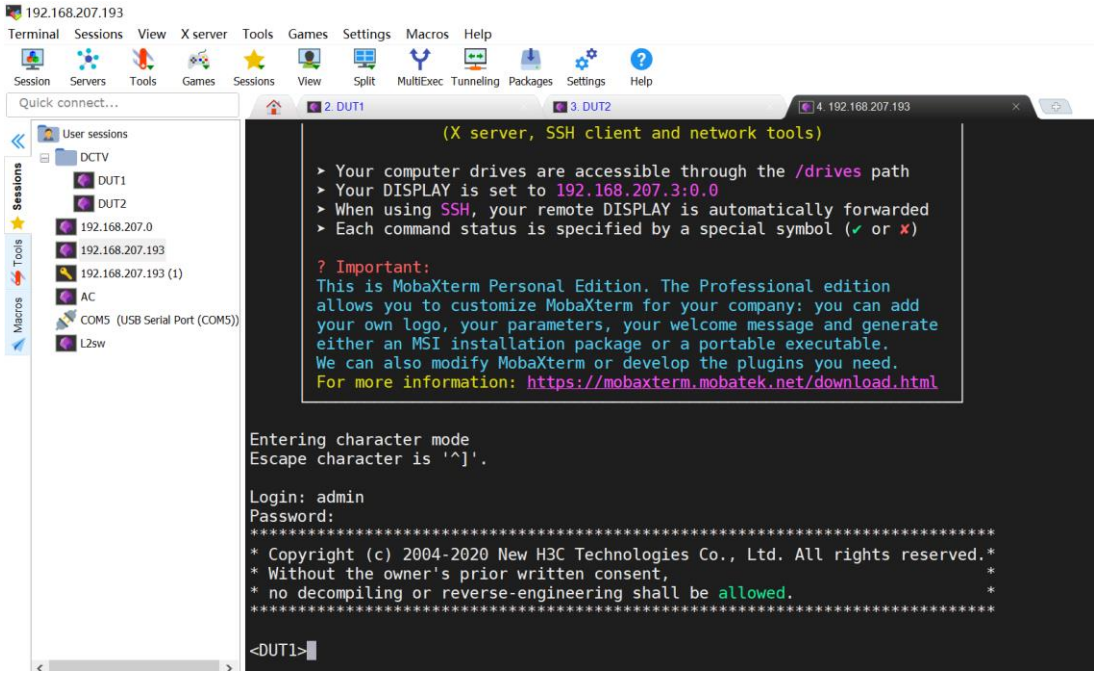
9. Use PC to access the device by telnet with Result 2



10. Configure the IP address 192.168.207.28 for PC



11. Use PC to access the device by telnet with Result 1



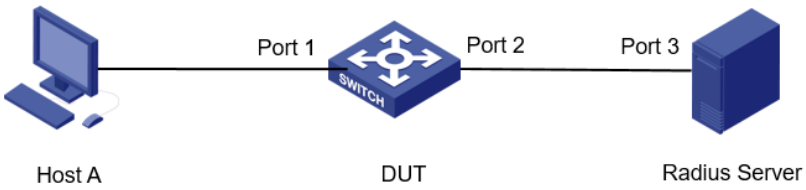
☐ Passed	☐ Failed

4.2 RADIUS authentication

Test Item Name: RADIUS authentication

Work Hour: 30 min

Test Topology:



Test Process:

Configure the RADIUS server correctly, add two accounts for the telnet users and specify the passwords for the accounts.

1. Telnet to the switch from Host A Enable the telnet server.
2. Enable scheme authentication for VTY line 0 to 63.
3. Enable the default user role feature.
4. Create a RADIUS scheme named *test*.
5. Specify the primary authentication and accounting servers.
6. Set the shared keys to expert in plaintext form for secure RADIUS communication.
7. Exclude domain names from the usernames sent to the RADIUS server.
8. Create an ISP domain named *test*.
9. Specify the ISP domain as the default ISP domain.
10. Configure the ISP domain to use RADIUS scheme test as the default authentication, authorization, and accounting methods.
11. Configure the RADIUS server correctly, add two accounts for the telnet users, and specify the passwords for the accounts.
12. Telnet to the switch from Host A and Host B, and enter the correct usernames and passwords. Result 1 is expected.
13. Telnet to the switch from Host A and Host B, and enter incorrect usernames and passwords. Result 2 is expected.

Expect Results:

1. The users can telnet to the switch from Host A and Host B.
2. The users cannot telnet to the switch from Host A or Host B.

Actual Result：

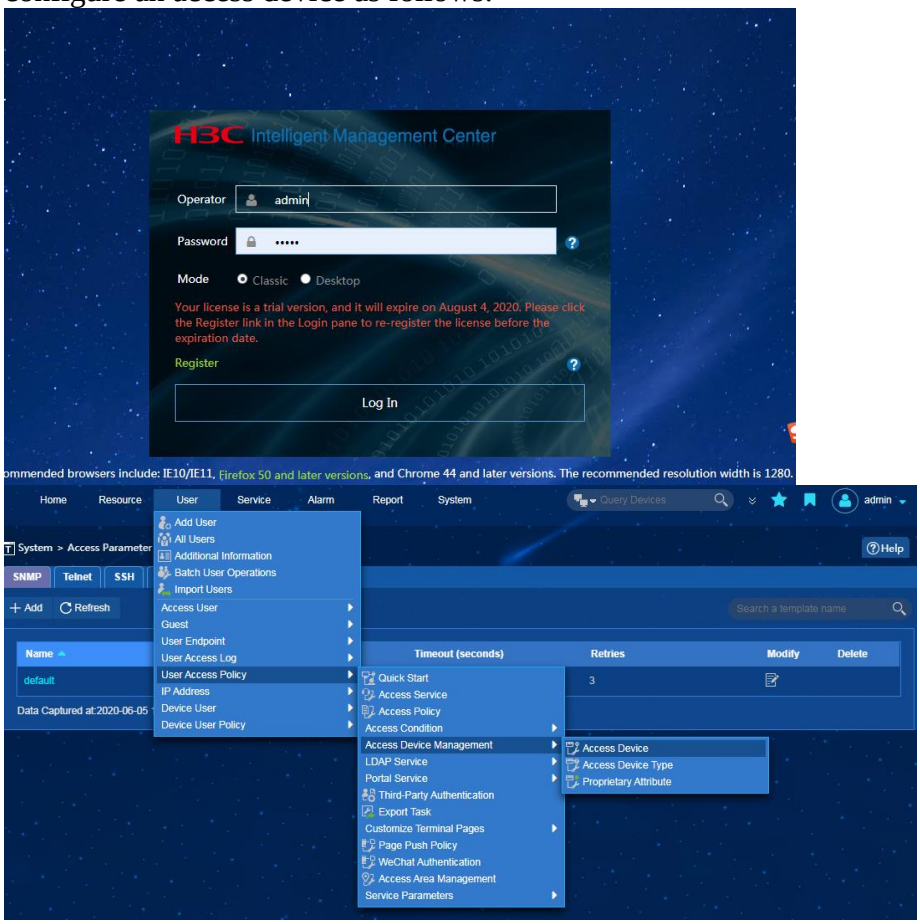
1. Configuration on DUT:

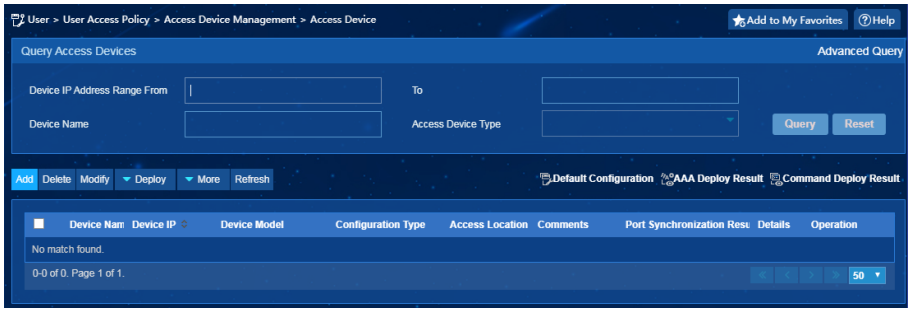
```
#
 telnet server enable
#
line vty 0 63
 authentication-mode scheme
 user-role network-admin
 user-role network-operator
#
 role default-role enable
#
radius scheme test
 primary authentication 192.168.207.57
 primary accounting 192.168.207.57
 key authentication simple expert
 key accounting simple expert
 user-name-format without-domain
 nas-ip 192.168.206.108
#
primary authentication 192.168.207.57
primary accounting 192.168.207.57
key authentication simple expert
key accounting simple expert
#
user-name-format without-domain
#
domain test
 authentication login radius-scheme test
 authorization login radius-scheme test
 accounting login radius-scheme test
#
```

2. Configuring the RADIUS server:

(1) Add the router to the IMC platform as an access device:

Log in to IMC, click the **User** tab, and select **User Access Policy** > **Access Device Management** > **Access Device** from the navigation tree. Then, click **Add** to configure an access device as follows:

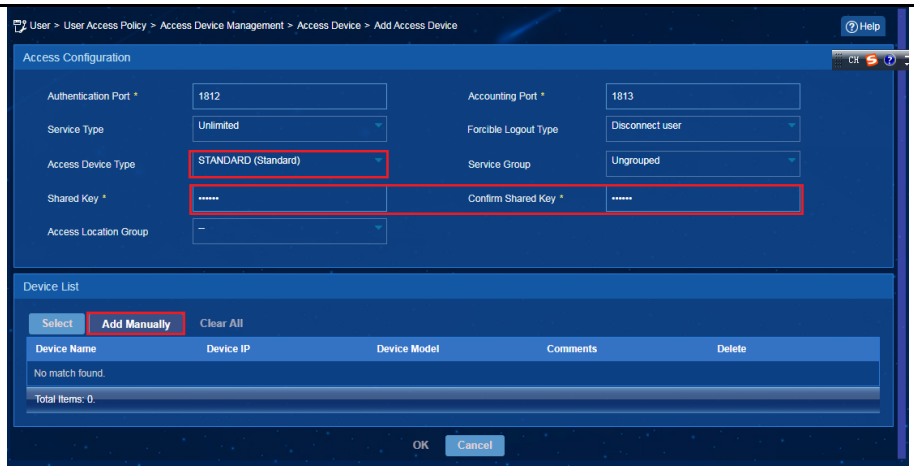




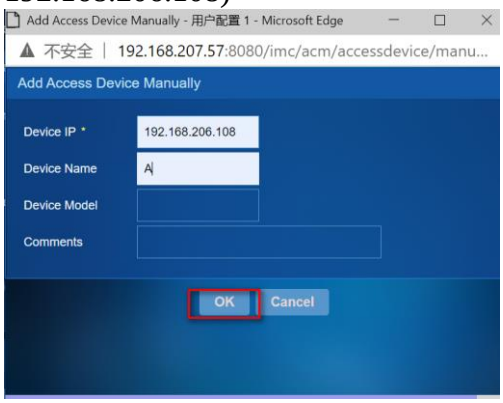
a. Set the shared key for secure RADIUS communication to **expert**.

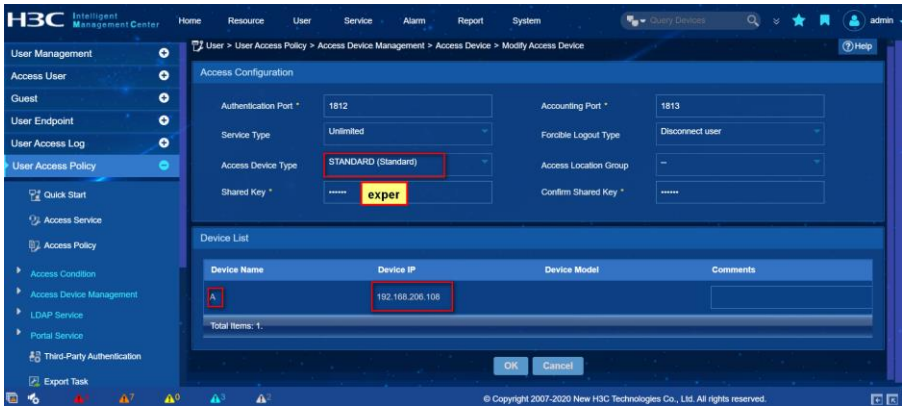
b. Set the ports for authentication and accounting to **1812** and **1813**, respectively.

c. Select **STANDARD (Standard)** from the **Access Device Type** list.



e. Select an access device from the device list or **manually add** an access device. In this example, the device IP address is 192.168.207.108. (equals to nas-ip address 192.168.206.108)

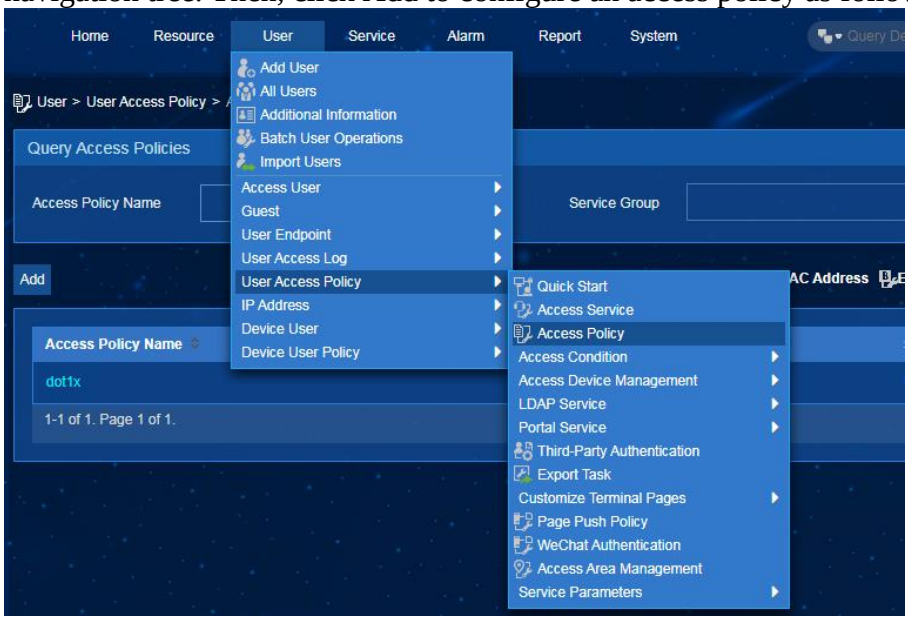


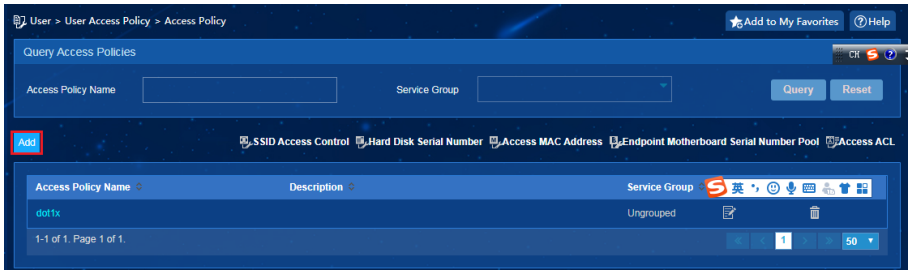


f. Use the default values for other parameters and click OK.
The IP address of the access device specified here must be the same as the source IP address of the RADIUS packets sent from the router. The source IP address is chosen in the following order on the router:
IP address specified by using the nas-ip command.
IP address specified by using the radius nas-ip command.
IP address of the outbound interface (the default).

(2) Add an access policy:

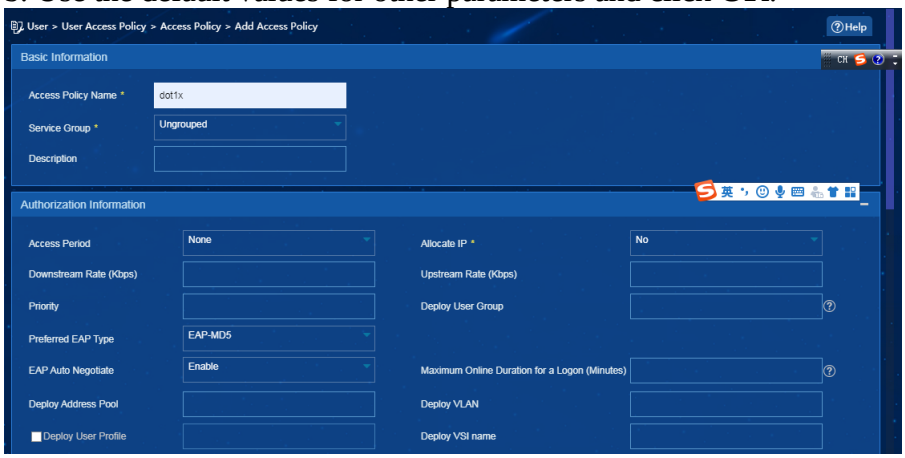
Click the User tab, and select **User Access Policy** > **Access Policy** from the navigation tree. Then, click Add to configure an access policy as follows:

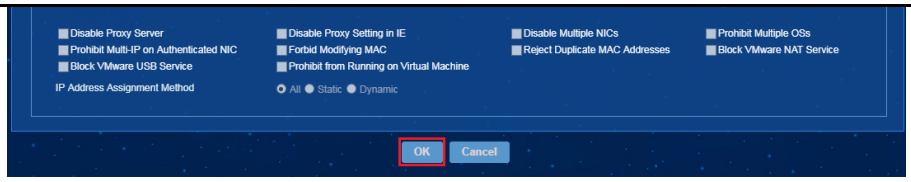


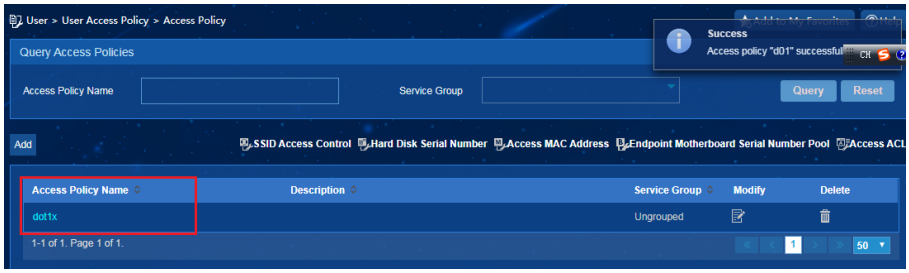


a. Enter Access Policy Name **dot1x**.

b. Use the default values for other parameters and click **OK**.

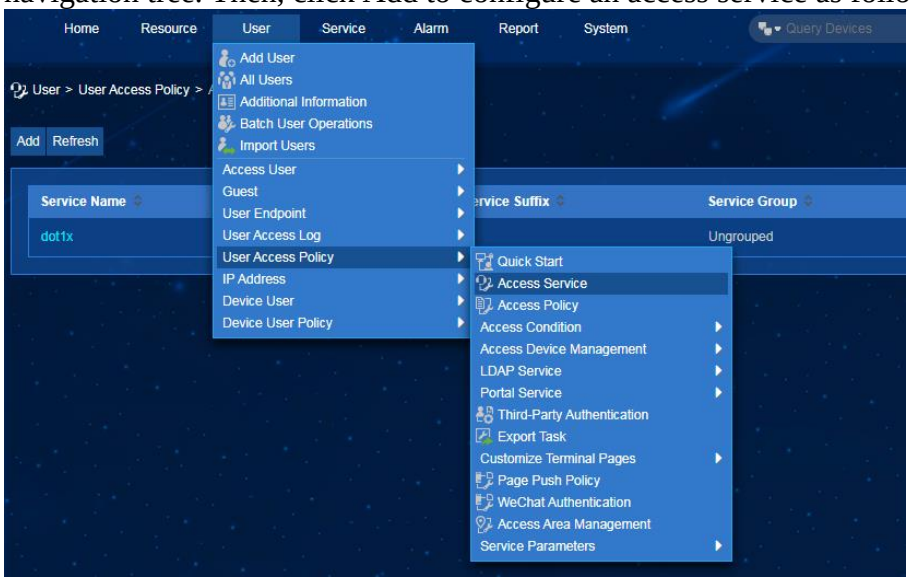






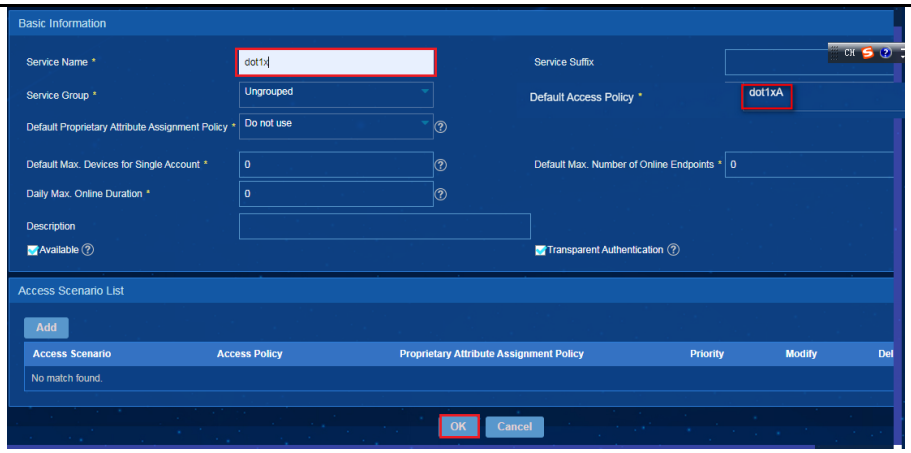
(3) Add an access service:

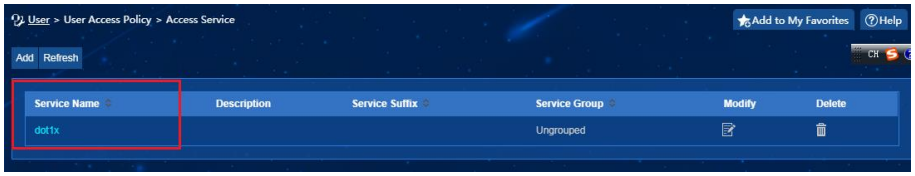
Click the User tab, and select **User Access Policy** > **Access Service** from the navigation tree. Then, click Add to configure an access service as follows:



a. Enter Service Name dot1x.

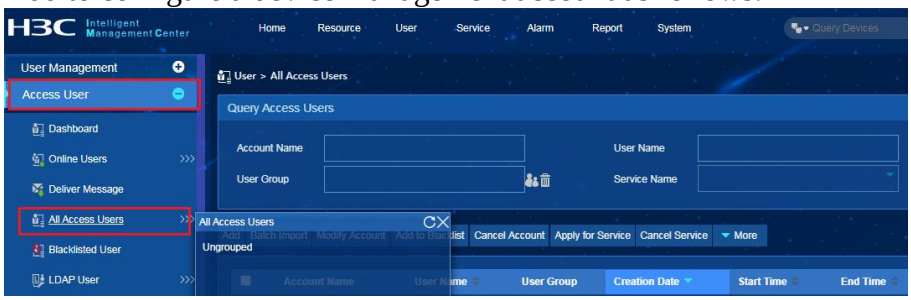
b. Use the default values for other parameters and click **OK**.

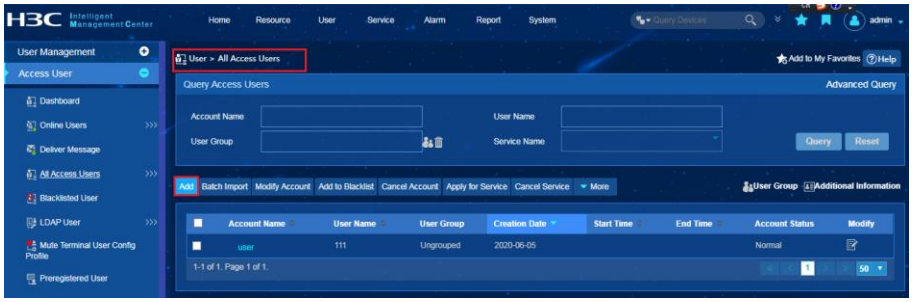




(4) Add an access user for device management:

Select Access User View > All Access Users from the navigation tree. Then, click Add to configure a device management account as follows:



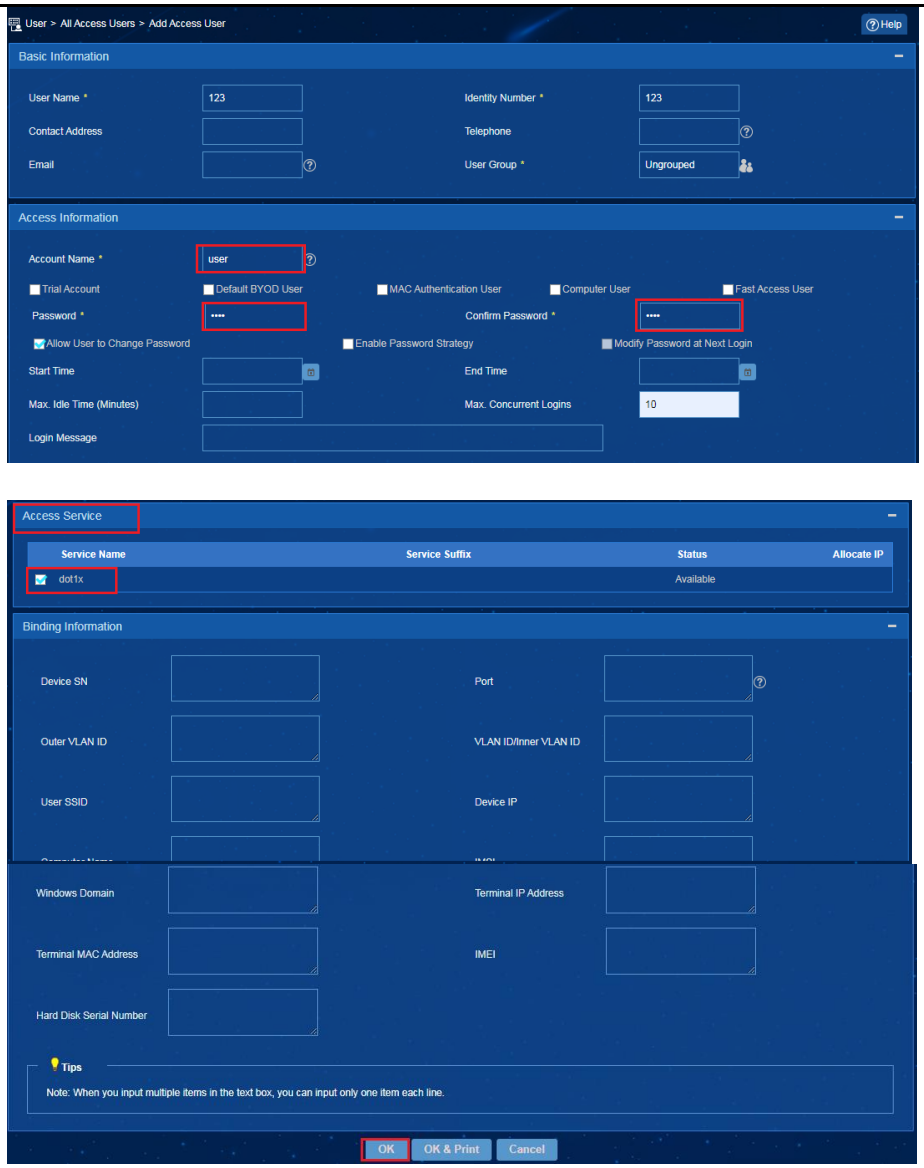


a. Enter account name **user** and specify the password as **1111** form the Access Information.

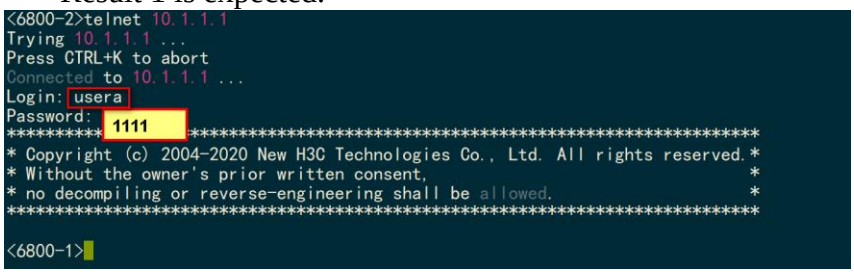
b. Specify 10 from the **Max Concurrent Logins** list.

c. Select the **dot1x** in Access Service.·

d. Click OK.



3. Telnet to the switch from PC 4, and enter the correct usernames and passwords. Result 1 is expected.



4. Telnet to the switch from PC 4, and enter incorrect usernames and passwords. Result 2 is expected.

```
Login: admin
Password:
E63018: The user does not exist or has not subscribed to this service.
AAA authentication failed.
Login: user
Password:
E63032: Incorrect password. You can retry 9 times.
AAA authentication failed.
Login:
```

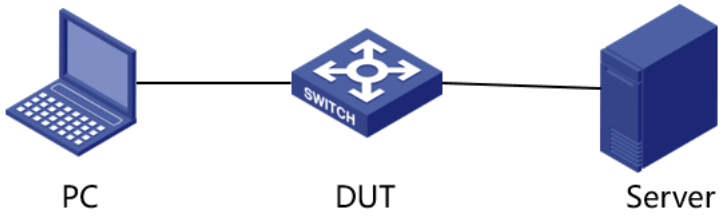
☐ Passed	☐ Failed

4.3 TACACS +

Test Item Name: TACACS +

Work Hour：30 min

Test Topology:



Test Process:

1. Add the DUT to the server as an AAA client. (Details not shown)
2. Add a Telnet user on the server. (Details not shown.)
3. Create and configure HWTACACS scheme hwtac on the DUT.
4. Create ISP domain hwtacacs and apply HWTACACS scheme hwtac to the ISP domain for authentication, authorization, and accounting of users.
5. Specify ISP domain hwtacacs as the default ISP domain.
6. Enable the Telnet server on the DUT and enable scheme authentication for Telnet users on VTY user lines 0 to 63.
7. Enable the default user role feature.
8. On the PC, use the correct username and password to log in to the DUT. Result 1 is expected.
9. On the PC, use the incorrect username or password to log in to the DUT. Result 2 is expected.

10. On the PC, use a username and password that do not exist on the server to log in to the DUT. Result 2 is expected.

Expect Results:

1. The PC successfully logs in to the DUT.
2. The PC cannot log in to the DUT.

Actual Result：

1. Enable Telnet server.

```
[DUT]telnet server enable
```

2. Enable scheme authentication for Telnet users on VTY user interfaces 1 through 15.

```
[DUT]line vty 0 63
[DUT-line-vty0-63]authentication-mode scheme
```

3. Enable the default user role feature.

```
[DUT]role default-role enable
```

4. Configure the HWTACACS scheme.

```
[DUT]hwtacacs scheme 1
[DUT-hwtacacs-1]primary authentication 192.168.207.53
[DUT-hwtacacs-1]primary authorization 192.168.207.53
[DUT-hwtacacs-1]primary accounting 192.168.207.53
[DUT-hwtacacs-1]key authentication simple 12345
[DUT-hwtacacs-1]key authorization simple 12345
[DUT-hwtacacs-1]key accounting simple 12345
[DUT-hwtacacs-1]user-name-format without-domain
[DUT-hwtacacs-1]nas-ip 192.168.207.193
```

5. Specify AAA schemes for the ISP domain.

```
[DUT]domain 1
[DUT-isp-1]authentication login hwtacacs-scheme 1
[DUT-isp-1]authorization login hwtacacs-scheme 1
[DUT-isp-1]accounting login hwtacacs-scheme 1
```

6. Specify the ISP domain example as the default domain.

```
[DUT]domain default enable 1
```

7. Configure the HWTACACS server:

The HWTACACS server runs IMC PLAT.

Add a shell profile.

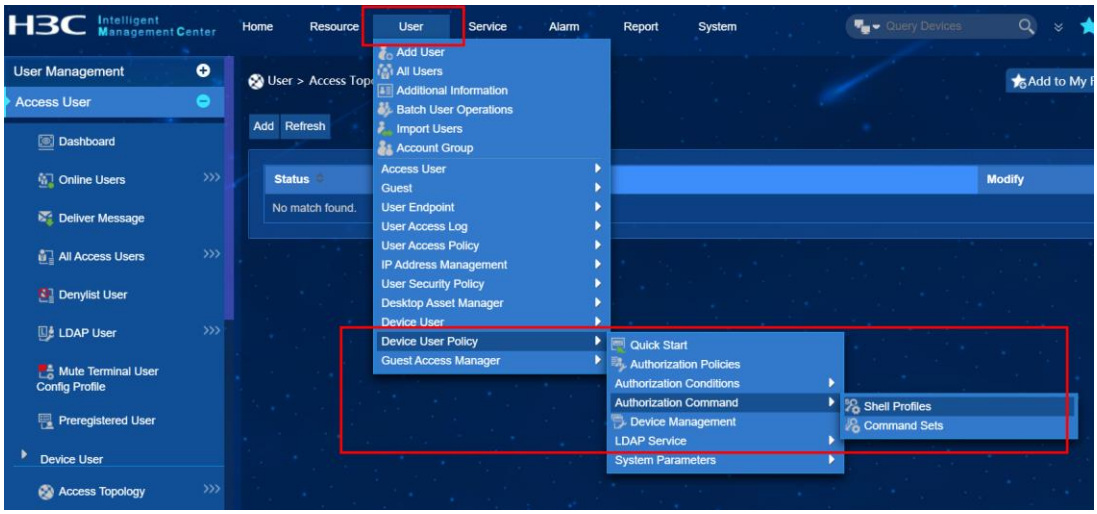
a. Log into IMC.

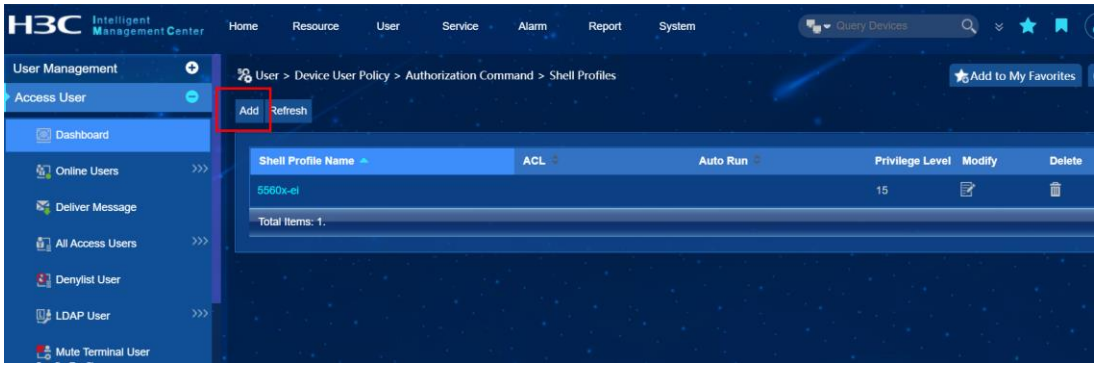
b. Click the User tab.

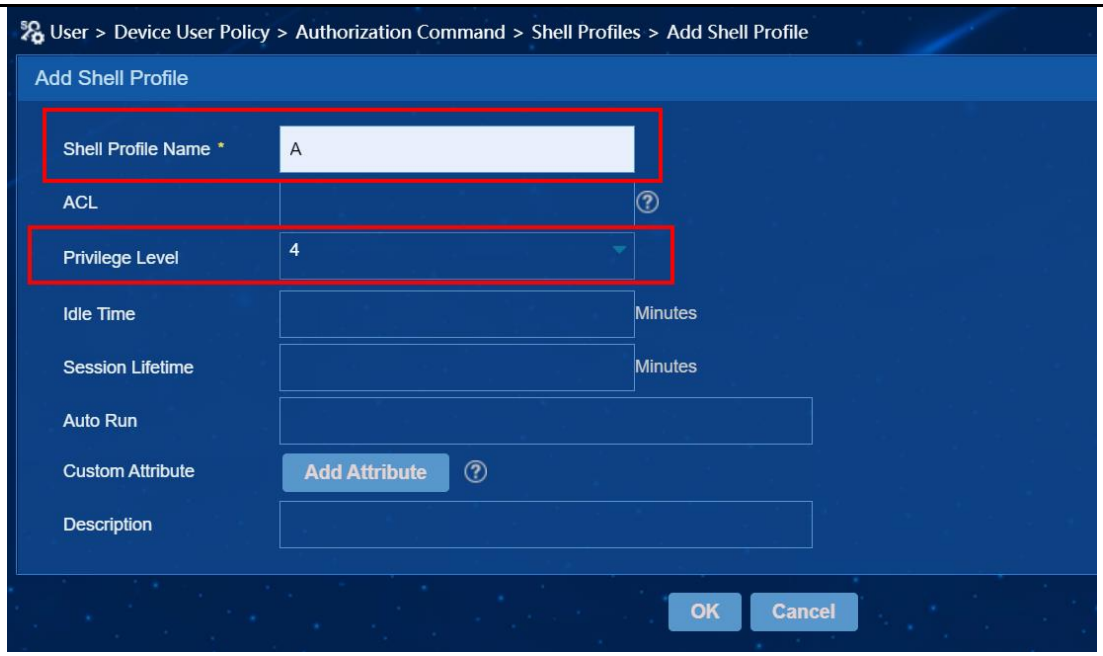
c. From the navigation tree, select Device User Policy > Authorization Command > Shell Profiles.

d. Click Add.

e. On the Add Shell Profile page, configure the shell profile name and the privilege level, and click OK.







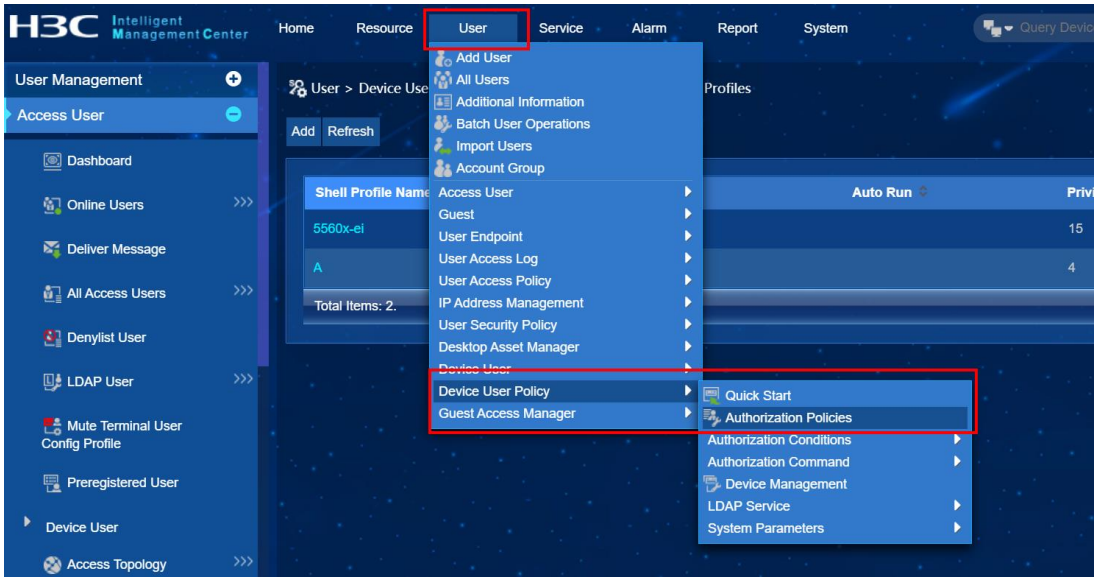
Add an authorization policy.

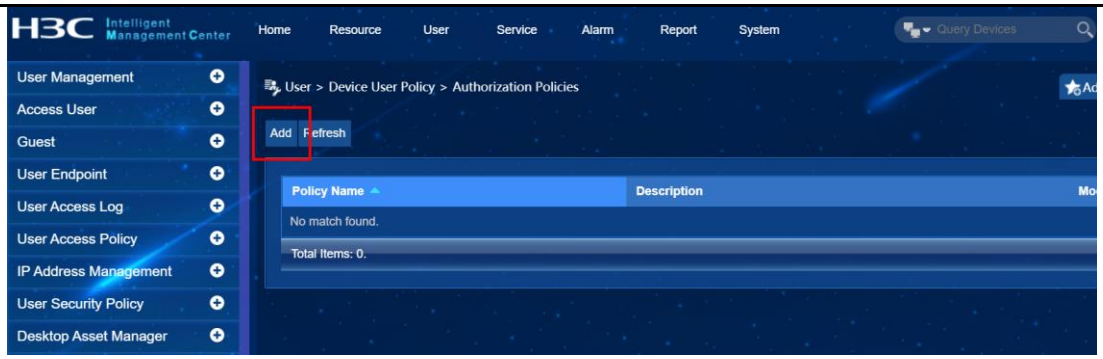
a. From the navigation tree, select Device User Policy > Authorization Policies.

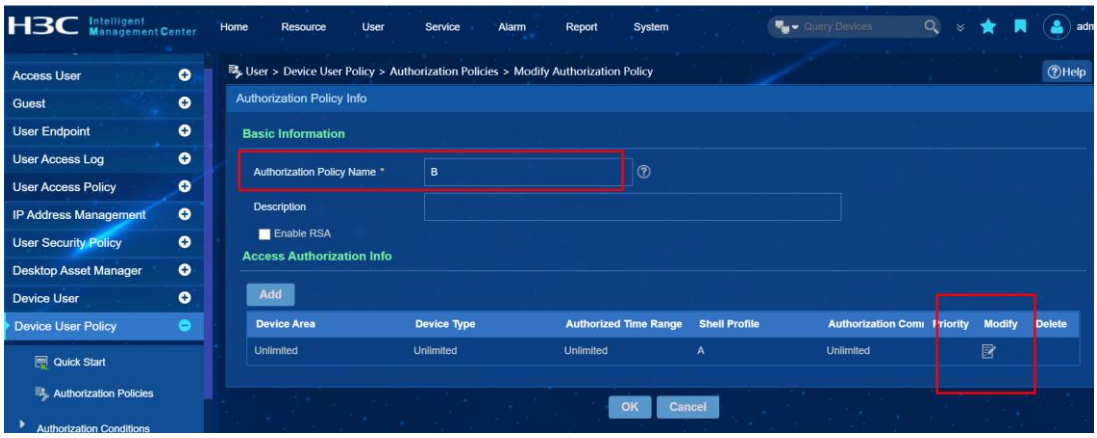
b. Click Add.

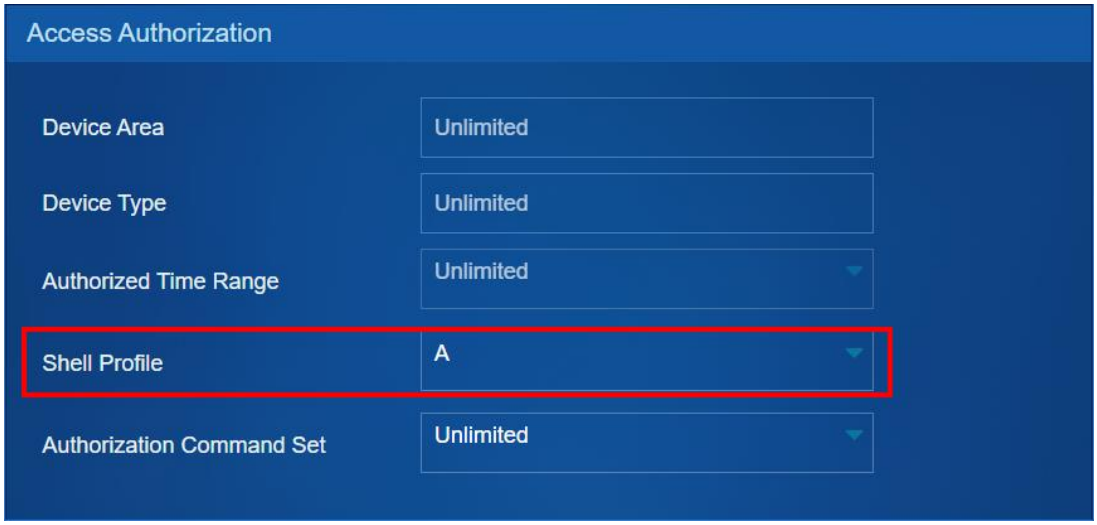
c. On the Add Authorization Policy page, configure the policy name and add the configured shell profile to the Access Authorization Info area.

d. Click OK.









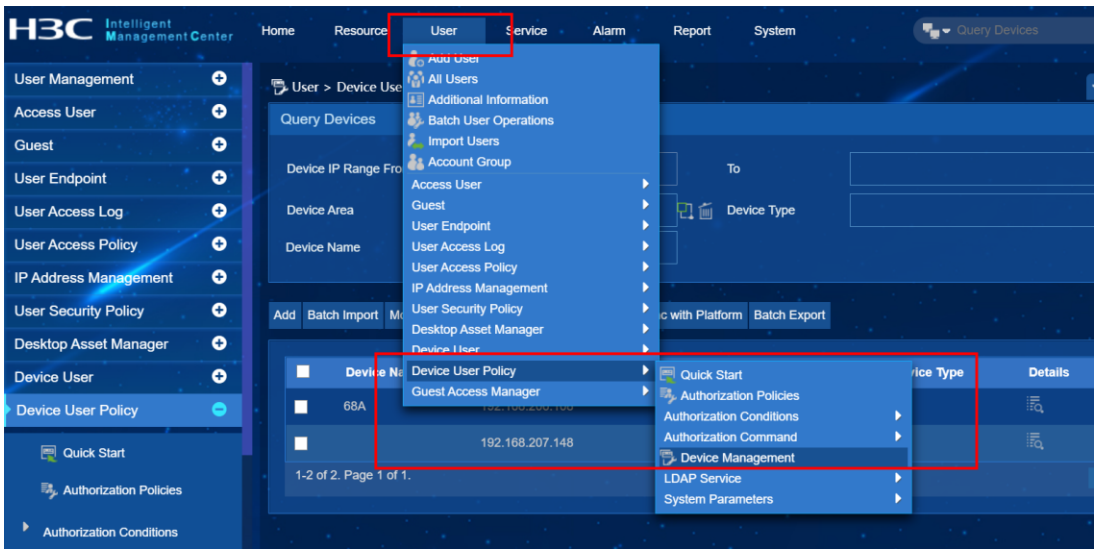
Add the DUT as an access device.

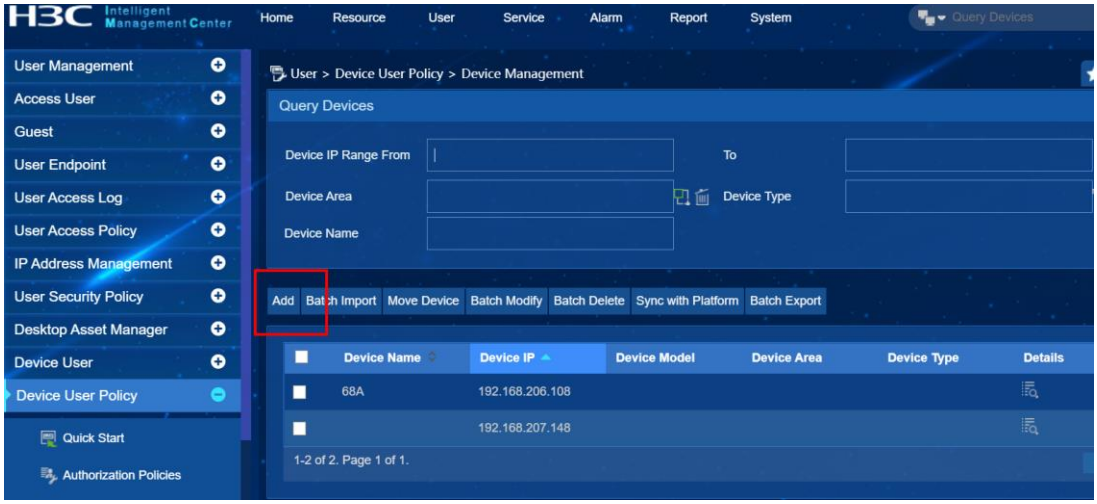
a. From the navigation tree, select Device User Policy > Device Management.

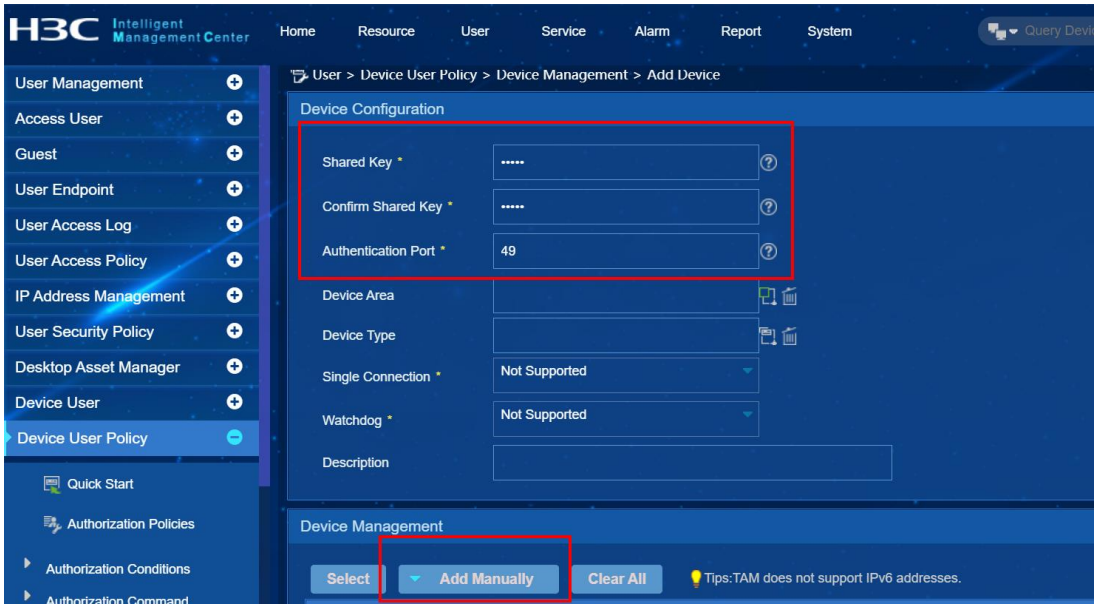
b. Click Add.

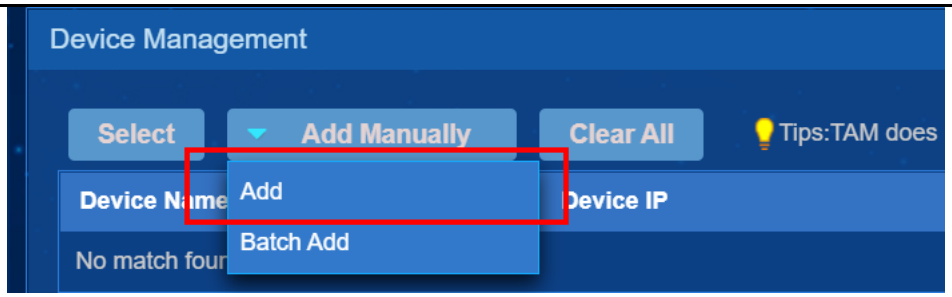
c. On the Add Device page, configure the shared key as expert and set the authentication port to 49. In the Device Management area, click Select or Add Manually to add the DUT to IMC as an access device.

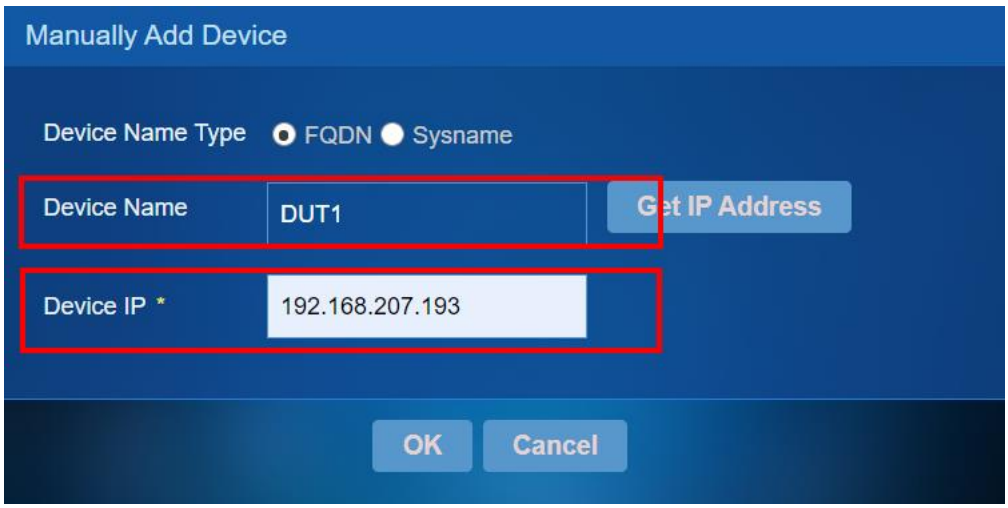
d. Click OK.











Add an access user.

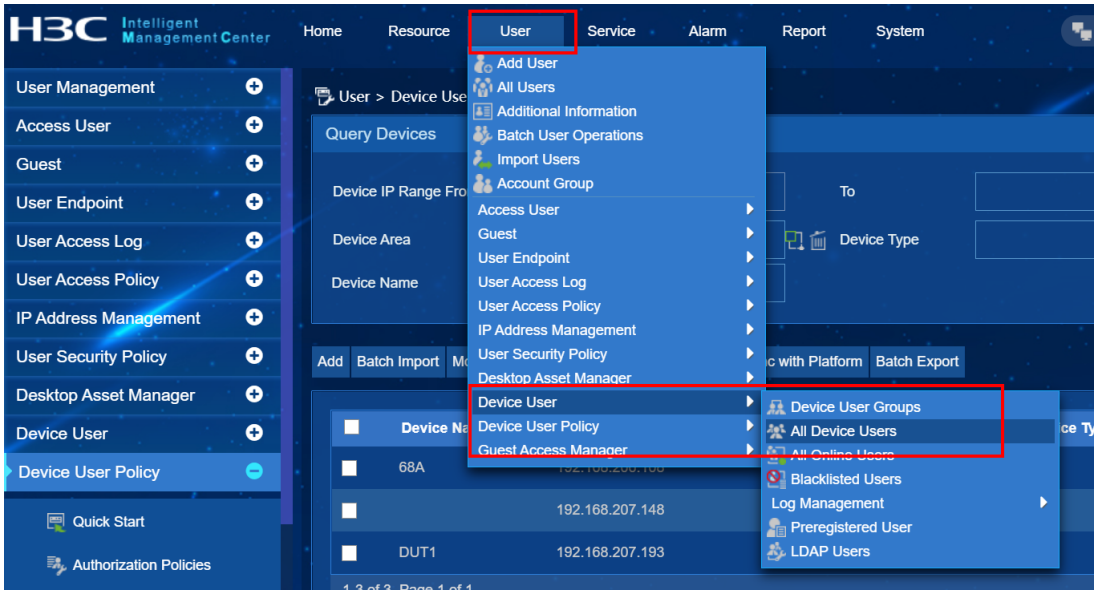
a. From the navigation tree, select Device User > All Device Users.

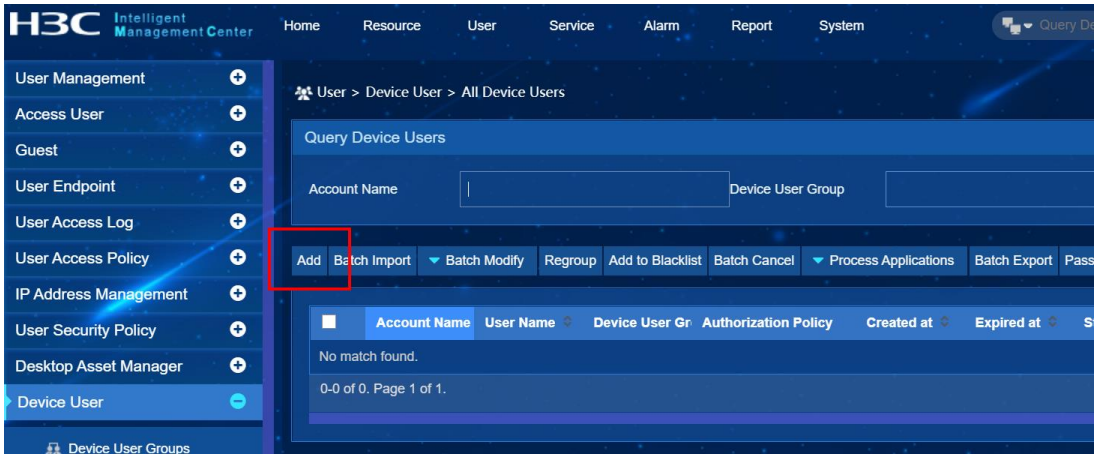
b. Click Add.

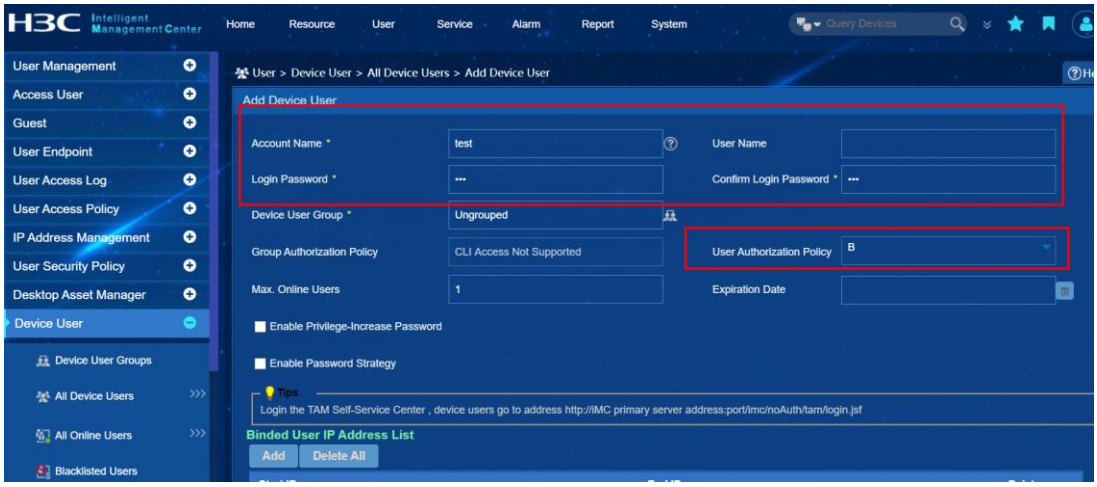
c. On the Add Device User page, add the user test and configure a password for the user.

d. Select the configured authorization policy from the User Authorization Policy list.

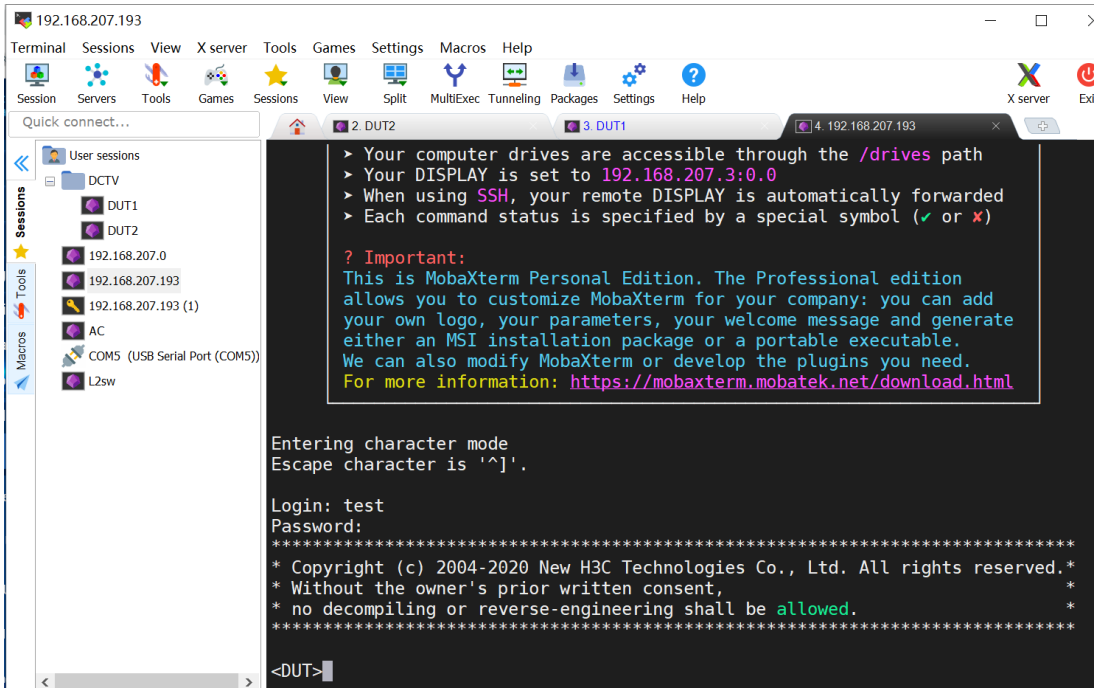
e. Click OK.







8. Host A uses the correct username and password to log into the DUT. Result 1 is expected.

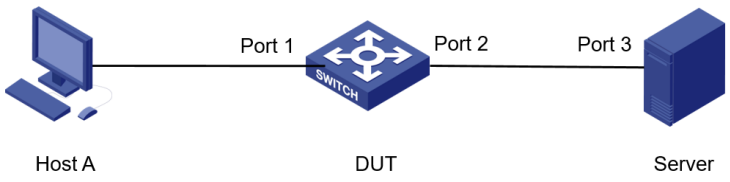


9. Host A uses incorrect usernames and passwords to log into the DUT. Result 2 is expected.

☐ Passed	☐ Failed

4.4 802.1X authentication

Test Item Name:802.1X authentication
Work Hour: 60 min
Test Topology:



Test Process:

1. Enable 802.1X globally on the DUT.
2. Enable 802.1X on the Port 1 (interface connected to the Client).
3. Create and configure RADIUS scheme test.
4. Create ISP domain test.com and apply RADIUS scheme test to the ISP domain for authentication, authorization, and accounting of LAN users.
5. On the DUT, assign Port 2 (interface connected to the RADIUS server) to VLAN 2 and assign IP address 192.168.207.53 to VLAN-interface 2.
6. On the RADIUS server at 192.168.207.53, add user user with password 1111, configure the authentication key as expert, and add IP address 13.1.1.3 of the DUT to the NAS IP list.
7. Use username user@h3c.com and password 1111 to initiate authentication from PC A.
8. Display user connection information. Result 1 is expected.
9. Ping the gateway address of PC A to verify the network accessibility of PC A. For example, the gateway of PC A is the VLAN interface of the VLAN to which Port 1 belongs. Ping the IP address of that VLAN interface. Result 2 is expected.
10. On the 802.1X client of PC A, disconnect the network.
11. Verify the network accessibility of PC A. Result 3 is expected

Expect Results:

1. The output shows that the user has passed 802.1X authentication, and it also shows the MAC address of PC A.
2. PC A can access the network.
3. PC A cannot access the network.

Actual Result：

1. Configuration on DUT

[DUT]dot1x

[DUT-GigabitEthernet1/0/1]dot1x

[DUT]radius scheme test

[DUT-radius-test]primary authentication 192.168.207.53 //the ip for 802.1X authentication server

[DUT-radius-test]primary accounting 192.168.207.53

[DUT-radius-test]key authentication simple expert

[DUT-radius-test]key accounting simple expert

[DUT-radius-test]user-name-format without-domain

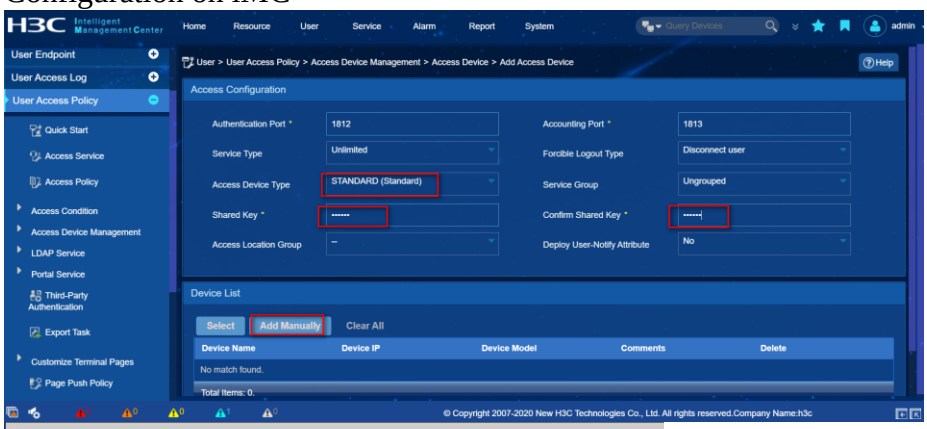
[DUT] domain test.com

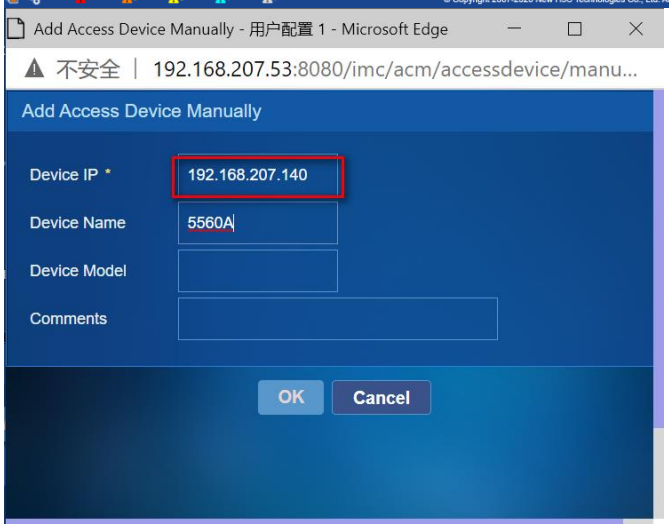
[DUT-isp-test.com] authentication lan-access radius-scheme test

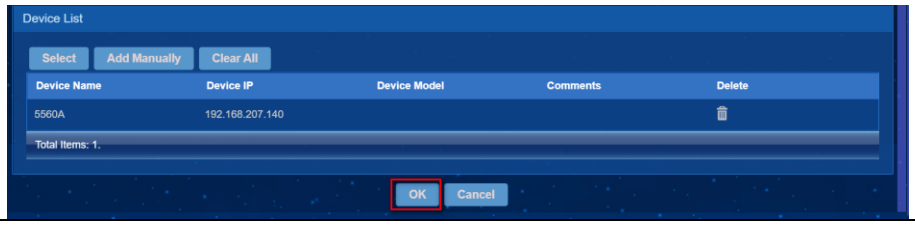
[DUT-isp-test.com] accounting lan-access radius-scheme test

[DUT-isp-test.com] authorization lan-access radius-scheme test

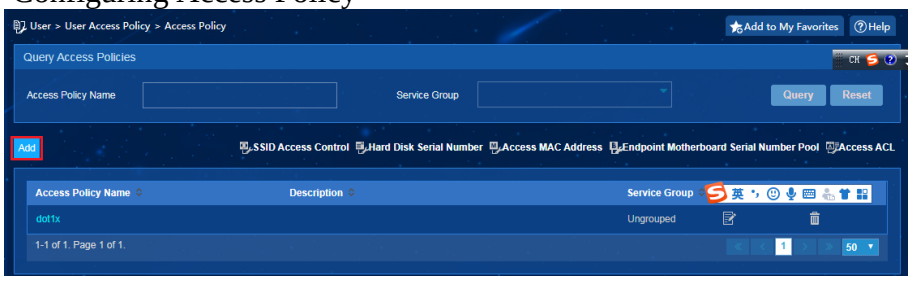
2. Configuration on iMC

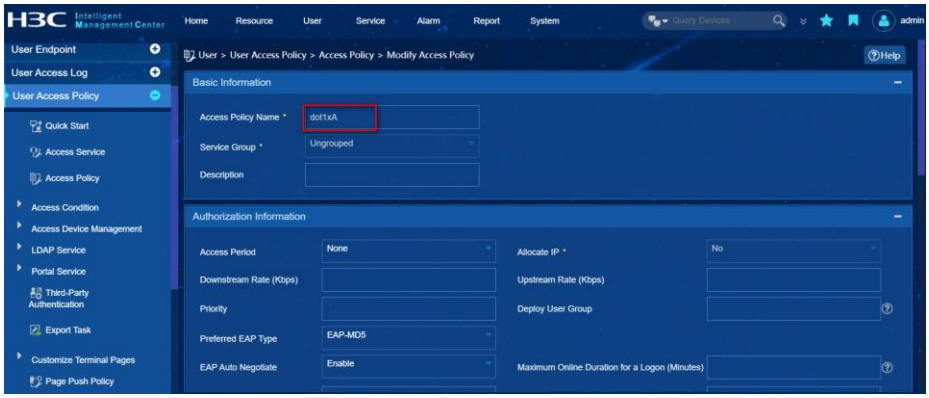


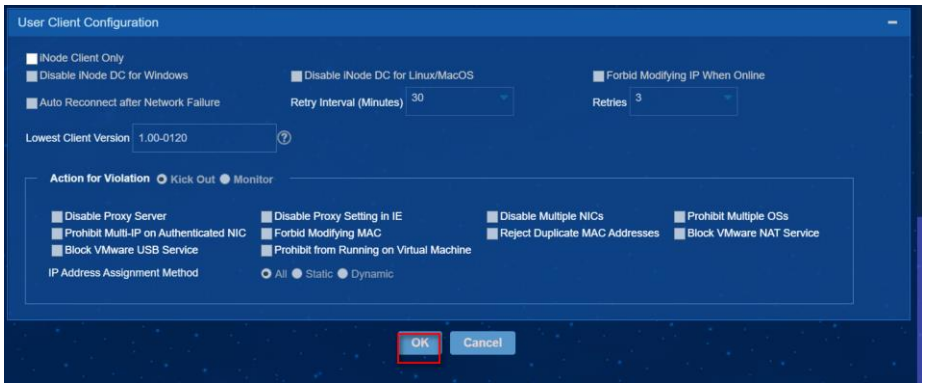


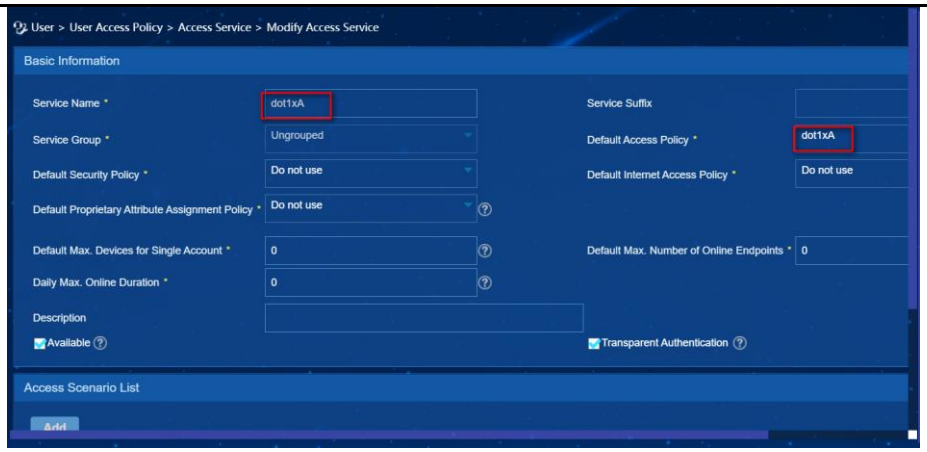


Configuring Access Policy









3. Use username user@h3c.com and password 1111 to initiate authentication from PC A.

4. Display user connection information.

```
[5560x-ei-1-GigabitEthernet1/0/5]dis dot1x sessions
 GigabitEthernet1/0/5   is link-up
   Online 802.1X users: 1
          MAC address       Auth state
          002b-6756-647f    Authenticated
 Ten-GigabitEthernet1/0/25   is link-up
   Online 802.1X users: 0
[5560x-ei-1-GigabitEthernet1/0/5]
```

5. Ping the gateway address of PC A to verify the network accessibility of PC A. For example, the gateway of PC A is the VLAN interface of the VLAN to

which Port 1 belongs. Ping the IP address of that VLAN interface.

```
C:\Users\j23223>ping 192.168.207.53

正在 Ping 192.168.207.53 具有 32 字节的数据:
来自 192.168.207.53 的回复: 字节=32 时间<1ms TTL=127
来自 192.168.207.53 的回复: 字节=32 时间<1ms TTL=127
来自 192.168.207.53 的回复: 字节=32 时间<1ms TTL=127
来自 192.168.207.53 的回复: 字节=32 时间=1ms TTL=127

192.168.207.53 的 Ping 统计信息:
    数据包: 已发送 = 4, 已接收 = 4, 丢失 = 0 (0% 丢失),
往返行程的估计时间(以毫秒为单位):
    最短 = 0ms, 最长 = 1ms, 平均 = 0ms
```

6. On the 802.1X client of PC A, disconnect the network.

7. Verify the network accessibility of PC A. Result 3 is expected.

```
C:\Users\j23223>ping 192.168.207.53

正在 Ping 192.168.207.53 具有 32 字节的数据:
来自 192.168.207.46 的回复: 无法访问目标主机。
来自 192.168.207.46 的回复: 无法访问目标主机。
来自 192.168.207.46 的回复: 无法访问目标主机。
来自 192.168.207.46 的回复: 无法访问目标主机。

192.168.207.53 的 Ping 统计信息:
    数据包: 已发送 = 4, 已接收 = 4, 丢失 = 0 (0% 丢失),
```

☐ Passed	☐ Failed

4.5 Syslog Server

Test Item Name: syslog server

Work Hour：20 min

Test Topology:

Test Process:

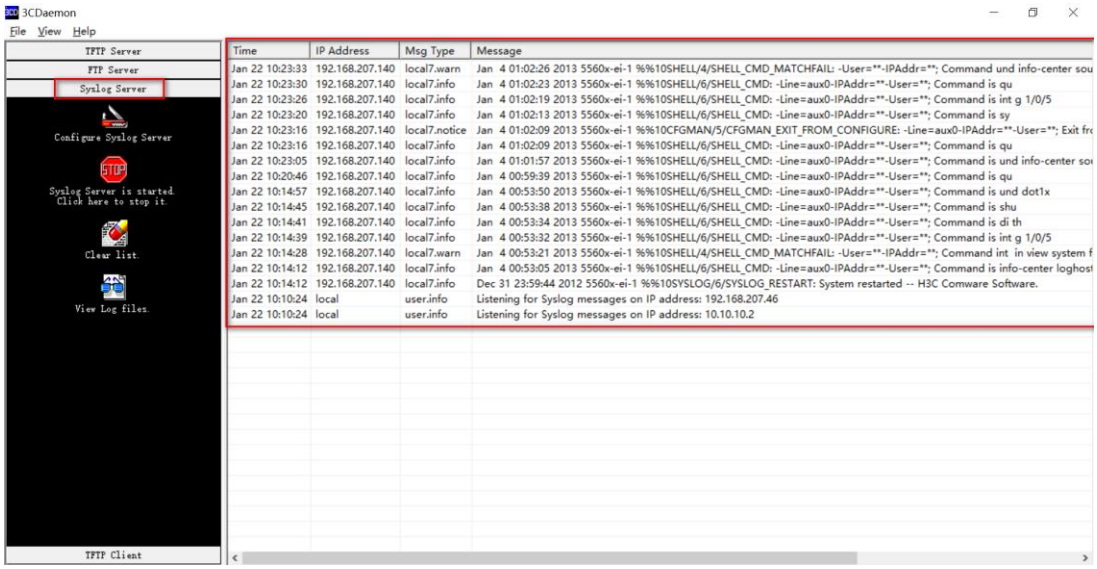
1. Configure the NMS VRF interface on DUT, and specify the source interface of syslog as VRF interface
2. Configure syslog server on DUT
3. Shutdown other Port on DUT and check whether the server can receive the log

Expect Results:

1. Interface up/down log is shown on the server

Actual Result：

1. Open the 3CD on computer and choose syslog Server



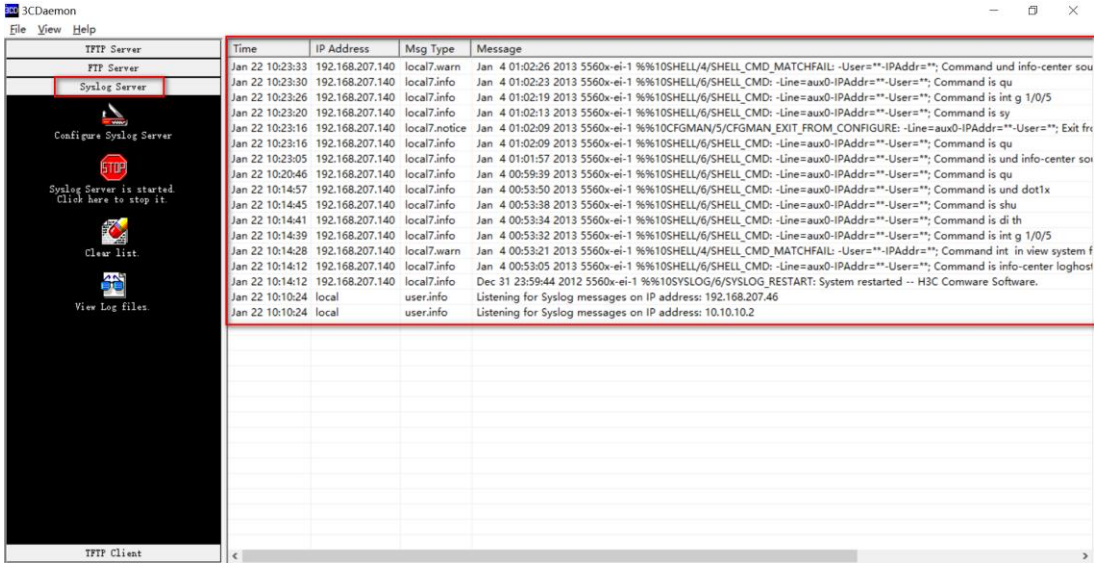
2. Configure syslog server on DUT

<Device>system-view

[Device]info-center enable

[Device]info-center loghost 192.168.207.46-------this is the computer's ip (this computer serves as syslog server)

3. Shutdown other Port on DUT and check whether the server can receive the log



☐ Passed	☐ Failed

4.6 FTP backup

Test Item Name: FTP backup of software and configuration file
Work Hour：20 min
Test Topology: 
Test Process: 1. Save the current configuration file named test.cfg. 2. Start the FTP service software on the PC, create a user, set the user name to "user" and the password to "test", and make sure that there are switch application files

in the directory where the service is set

3. Enter the command in the user view for FTP connection, and enter the correct user name and password to log in, you can get the result 1.
4. Ensure that there is a configuration file in Flash, execute the put command to upload the configuration file to the PC, and the expected result is 2.
5. Use the "display boot-loader" command to view the currently used software.
6. According to the startup software queried in the previous step (there may be multiple bin files), use the put command multiple times to upload the software file, and the expected result is 2. (Note to use binary transmission method to download)
7. Enter the quit command or the bye command to log out, Expected result 3.

Expect Results:

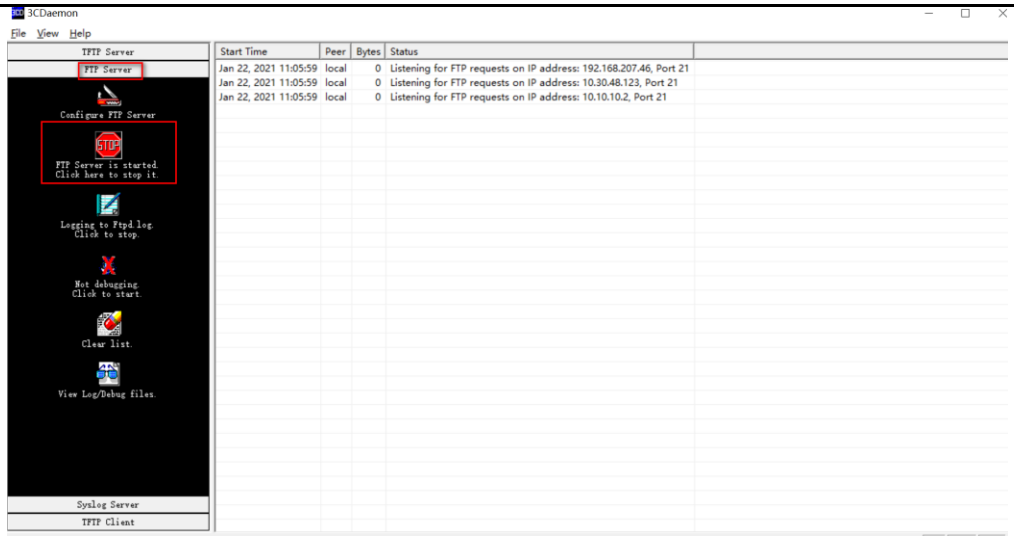
1. Login successful.
2. File upload completed.
3. Log out and disconnect.

Actual Result:

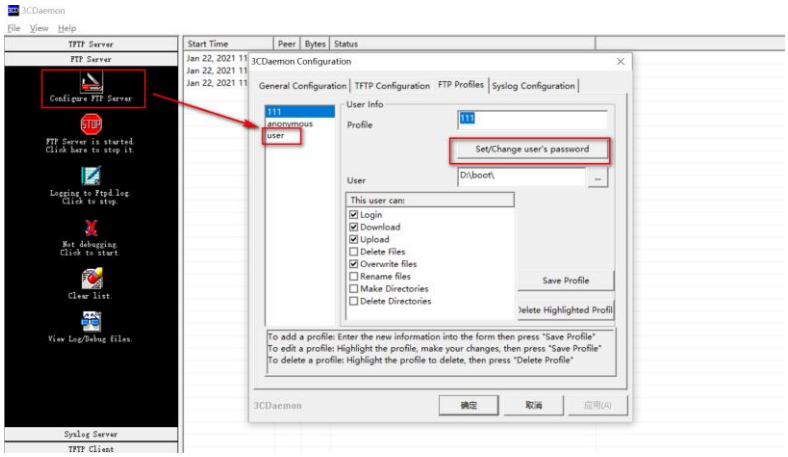
1. Save the test.cfg.

```
[5560x-ei-1]save
The current configuration will be written to the device. Are you sure? [Y/N]:y
Please input the file name(*.cfg)[flash:/j1x+m.cfg]
(To leave the existing filename unchanged, press the enter key):test.cfg
Validating file. Please wait...
Saved the current configuration to mainboard device successfully.
[5560x-ei-1]
```

2. Start the FTP service software on the PC.



Open the FTP server softer ware on computer, create a user, set the user name to "user" and the password to "test"



3. Enter the command in the user view for FTP connection, and enter the correct user name and password to log in.

```
<5560x-ei-1>ftp 192.168.207.46
Press CTRL+C to abort.
Connected to 192.168.207.46 (192.168.207.46).
220 3Com 3CDaemon FTP Server Version 2.0
User (192.168.207.46:(none)): user
331 User name ok, need password
Password:
230 User logged in
Remote system type is UNIX.
Using binary mode to transfer files.
ftp>
```

4. Execute the put command to upload the configuration file to the PC.

```
ftp> ?
Commands may be abbreviated.  Commands are:

append          delete          ls              quit            rmdir
ascii           debug           mkdir           reget           status
binary          dir             newer           rstatus         system
bye             disconnect      open            rhelp           user
cd              get             passive         rename          verbose
cdup            help            put             reset           ?
close           lcd             pwd             restart
```

```
ftp> put test.cfg
227 Entering passive mode (192,168,207,46,218,195)
125 Using existing data connection
.
226 Closing data connection; File transfer successful
4696 bytes sent in 0.002 seconds (2.26 Mbytes/s)
ftp>
```

5. Use the "display boot-loader" command to view the currently used software.

```
<5560x-ei-1>dis boot-loader
Software images on slot 1:
Current software images:
  flash:/s5560x_ei-cmw710-boot-f6517.bin
  flash:/s5560x_ei-cmw710-system-f6517.bin
  flash:/s5560x_ei-cmw710-freeradius-f6517.bin
  flash:/s5560x-ei-cmw710-escan-f6517.bin
Main startup software images:
  flash:/s5560x_ei-cmw710-boot-f6517.bin
  flash:/s5560x_ei-cmw710-system-f6517.bin
  flash:/s5560x_ei-cmw710-freeradius-f6517.bin
  flash:/s5560x-ei-cmw710-escan-f6517.bin
Backup startup software images:
  None
```

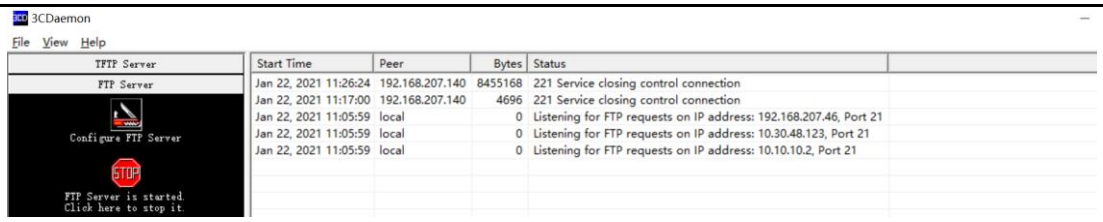
6. Use the put command multiple times to upload the software file.

```
<5560x-ei-1>ftp 192.168.207.46
Press CTRL+C to abort.
Connected to 192.168.207.46 (192.168.207.46).
220 3Com 3CDaemon FTP Server Version 2.0
User (192.168.207.46:(none)): user
331 User name ok, need password
Password:
230 User logged in
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> put s5560x_ei-cmw710-devkit-f6517.bin
227 Entering passive mode (192,168,207,46,219,184)
125 Using existing data connection
.................
226 Closing data connection; File transfer successful.
8455168 bytes sent in 10.227 seconds (807.34 Kbytes/s)
ftp>
```

7. Enter the quit command or the bye command to log out.

```
ftp> bye
221 Service closing control connection
<5560x-ei-1>
```

syslog appears in the FTP server.



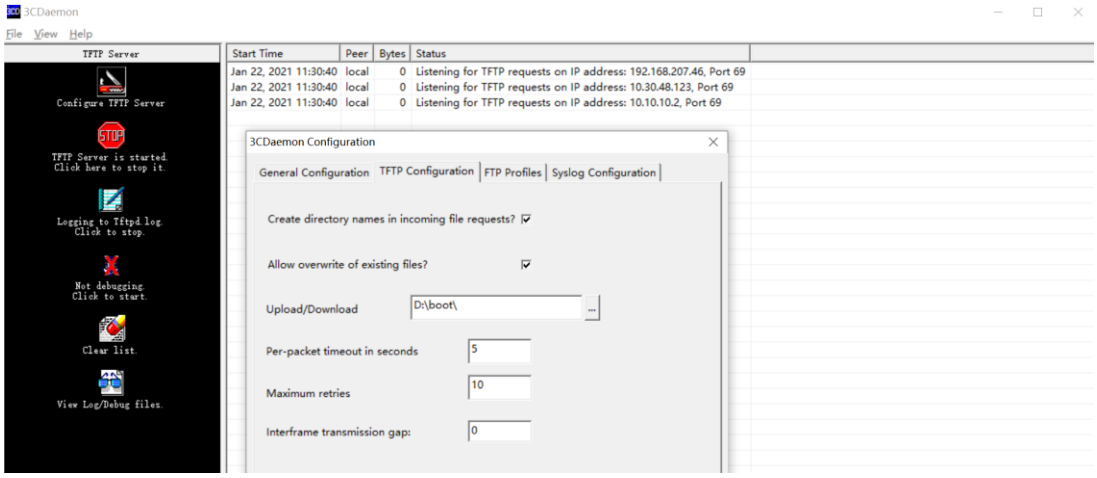
☐ Passed	☐ Failed

4.7 TFTP backup

Test Item Name: TFTP backup of software and configuration file
Work Hour：20 min
Test Topology: 
Test Process: 1. Save the current configuration file, named test.cfg. 2. Open the TFTP server program on the PC and set the file transfer path. 3. Ensure that there is a configuration file in Flash, execute the put command to upload the configuration file to the PC, and the expected result is 1. 4. Use the "display boot-loader" command to view the currently used software. 5. According to the startup software queried in the previous step (there may be multiple bin files), use the put command multiple times to upload the software file, and the expected result is 1. (Note to use binary transmission method to download)
Expect Results: 1. File upload completed. 2. File upload completed.
Actual Result： 1. Save the test.cfg.

```
[5560x-ei-1]save
The current configuration will be written to the device. Are you sure? [Y/N]:y
Please input the file name(*.cfg)[flash:/j1x+m.cfg]
(To leave the existing filename unchanged, press the enter key):test.cfg
Validating file. Please wait...
Saved the current configuration to mainboard device successfully.
[5560x-ei-1]
```

2. Open the TFTP server program on the PC and set the file transfer path.



3. Enxecute the put command to upload the configuration file to the PC.

```
<5560x-ei-1>tftp 192.168.207.46 put flash:/test.cfg
Press CTRL+C to abort.
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100  4696     0     0  100  4696      0  51750 --:--:-- --:--:-- --:--:-- 78266

<5560x-ei-1>
```

4. Use the "display boot-loader" command to view the currently used software.

```
<5560x-ei-1>dis boot-loader
Software images on slot 1:
Current software images:
  flash:/s5560x_ei-cmw710-boot-f6517.bin
  flash:/s5560x_ei-cmw710-system-f6517.bin
  flash:/s5560x_ei-cmw710-freeradius-f6517.bin
  flash:/s5560x-ei-cmw710-escan-f6517.bin
Main startup software images:
  flash:/s5560x_ei-cmw710-boot-f6517.bin
  flash:/s5560x_ei-cmw710-system-f6517.bin
  flash:/s5560x_ei-cmw710-freeradius-f6517.bin
  flash:/s5560x-ei-cmw710-escan-f6517.bin
Backup startup software images:
  None
<5560x-ei-1>
```

5. Use the *put* command multiple times to upload the software file.

```
<5560x-ei-1>tftp 192.168.207.46 put s5560x_ei-cmw710-devkit-f6517.bin
Press CTRL+C to abort.
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
  0 8257k     0     0     0 12800      0   2458  0:57:19  0:00:05  0:57:14  2490
```

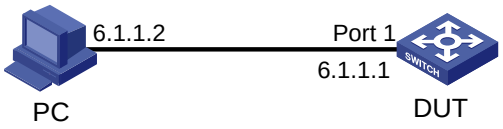
☐ Passed	☐ Failed

4.8 SNMPv2c

Test Item Name: SNMPv2c

Work Hour: 10 min

Test Topology:



Test Process:

1. Enable the SNMP agent.
2. Enable all SNMP versions.
3. Create an SNMP read-only community named public and read-write community named private.
4. On the MIB browser of the PC, use SNMPv2c to access the DUT and request the value of MIB object sysObjectID. Result 1 is expected.

Expect Results:

1. The MIB browser can obtain the value of sysObjectID through SNMPv2c successfully.

Actual Result:

1. Enable the SNMP agent

```
[DUT]snmp-agent
```

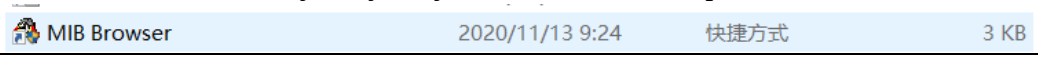
2. Enable all SNMP versions

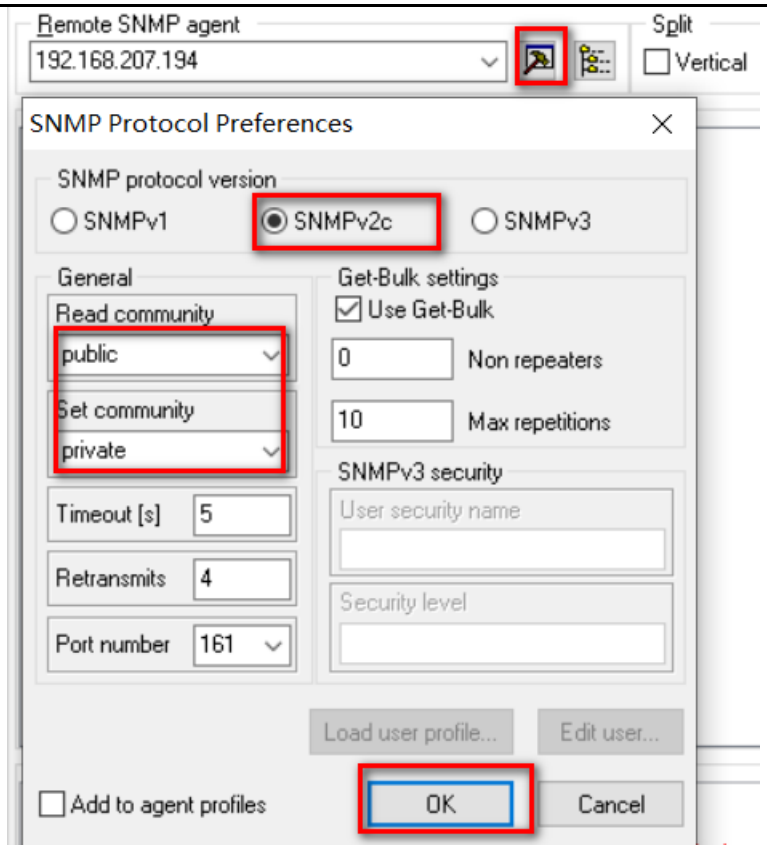
```
[DUT]snmp-agent sys-info version all
```

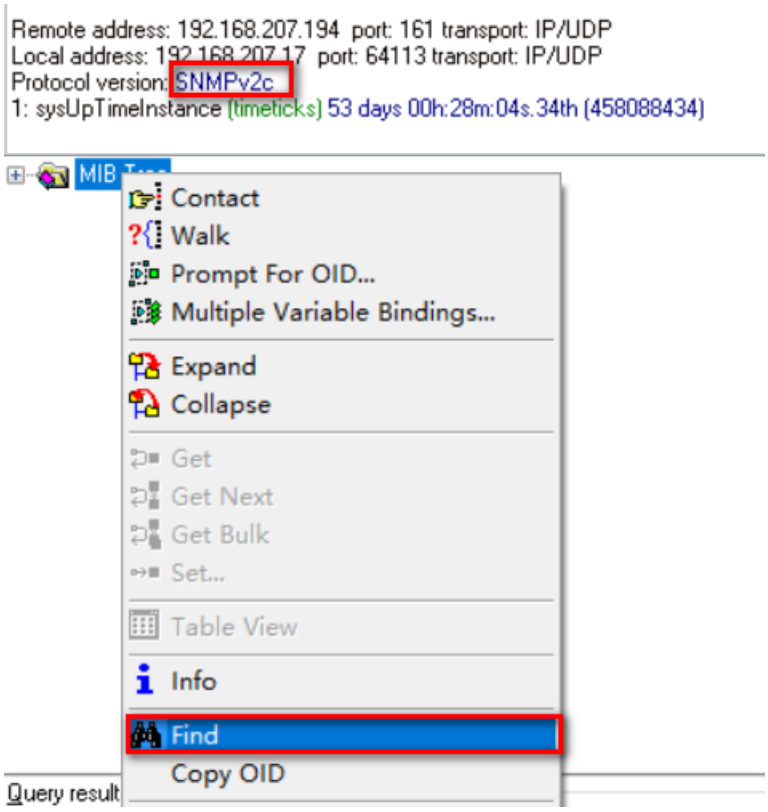
3. Create an SNMP read-only community named public and read-write community named private

```
[DUT]snmp-agent community read public
[DUT]snmp-agent community write private
```

4. On the MIB browser of the PC, use SNMPv2c to access the DUT and request the value of MIB object sysObjectID. Result 1 is expected

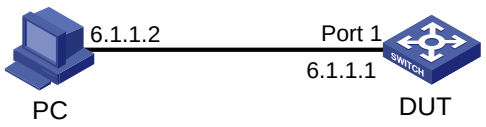



Remote SNMP agent
192.168.207.194
Split
Vertical
SNMP Protocol Preferences
SNMP protocol version
SNMPv1
SNMPv2c
SNMPv3
General
Read community
public
Set community
private
Timeout [s]
5
Retransmits
4
Port number
161
Get-Bulk settings
Use Get-Bulk
0
Non repeaters
10
Max repetitions
SNMPv3 security
User security name
Security level
Load user profile...
Edit user...
Add to agent profiles
OK
Cancel


Remote address: 192.168.207.194 port: 161 transport: IP/UDP
Local address: 192.168.207.17 port: 64113 transport: IP/UDP
Protocol version: SNMPv2c
1: sysUpTimeInstance (timeticks) 53 days 00h:28m:04s.34th (458088434)
MIB
Contact
Walk
Prompt For OID...
Multiple Variable Bindings...
Expand
Collapse
Get
Get Next
Get Bulk
Set...
Table View
Info
Find
Copy OID
Query result

☐ Passed	☐ Failed

4.9 SNMP Traps

Test Item Name: SNMP Traps
Work Hour: 10 min
Test Topology: 
Test Process: 1. Enable SNMP Trap. 2. Configure DUT to support SNMPv1 access.

3. Create an SNMP read-only community named public and read-write community named private.
4. Configure the SNMP 2 Trap receiver.
5. Simulate to generate Trap event, result 1 is expected.

Expect Results:

1. The trap information could be seen on MIB Brower.

Actual Result:

1. Enable SNMP Trap.

```
[DUT]snmp-agent
[DUT]snmp-agent trap enable
```

2. Configure DUT to support SNMPv1 access.

```
[DUT]snmp-agent sys-info version v1
```

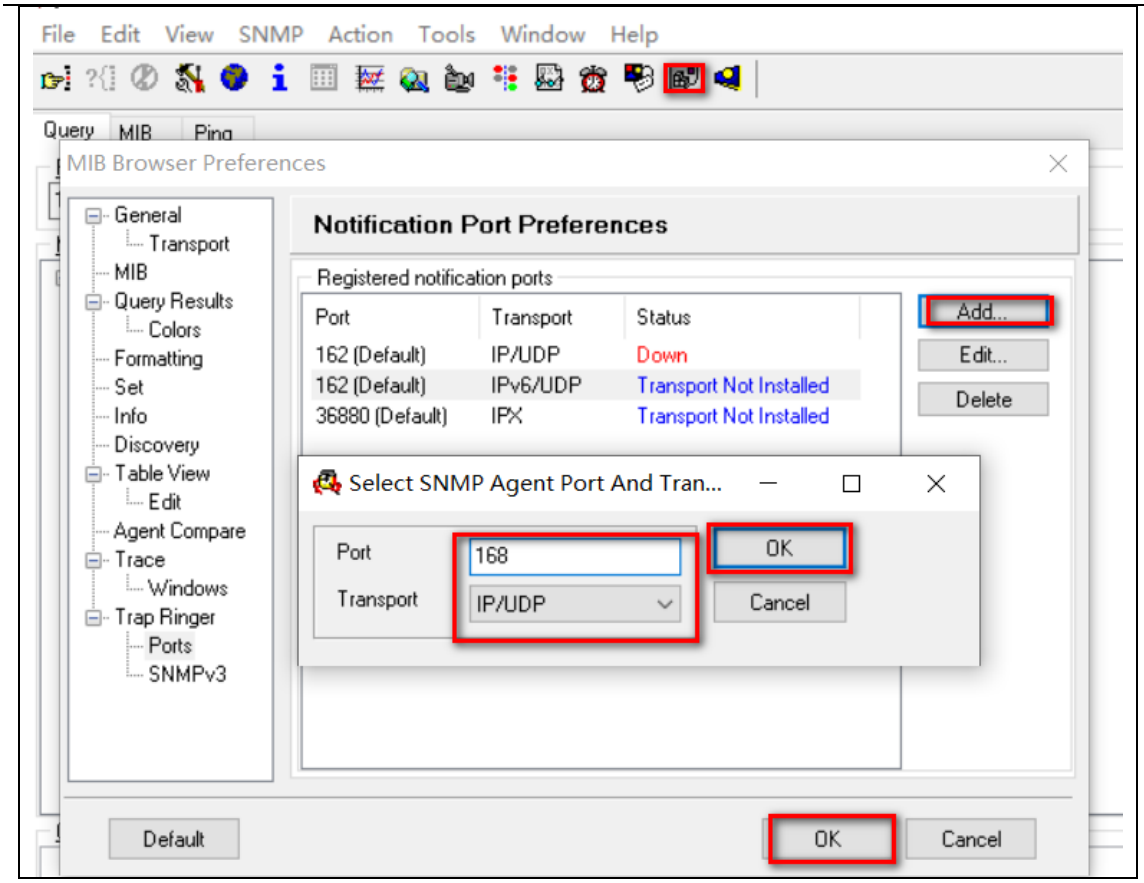
3. Create an SNMP read-only community named public and read-write community named private.

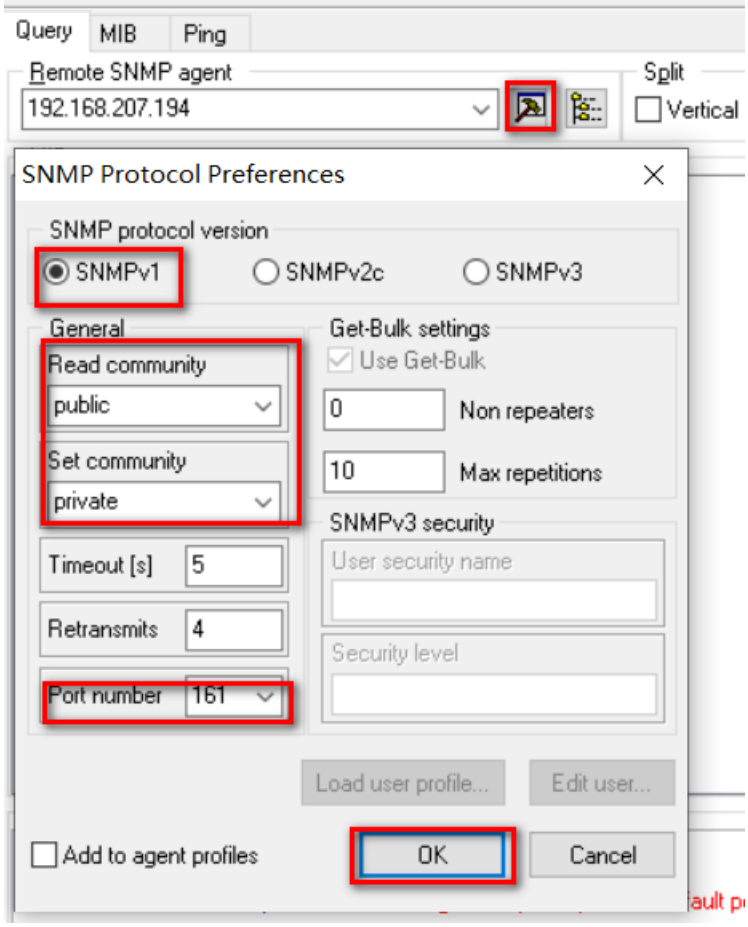
```
[DUT]snmp-agent community read public
[DUT]snmp-agent community write private
```

4. Configure the SNMP Trap receiver.

```
[DUT]snmp-agent  target-host trap address  udp-domain 192.168.207.17 udp-port 16
8 params securityname  public1 v1
```

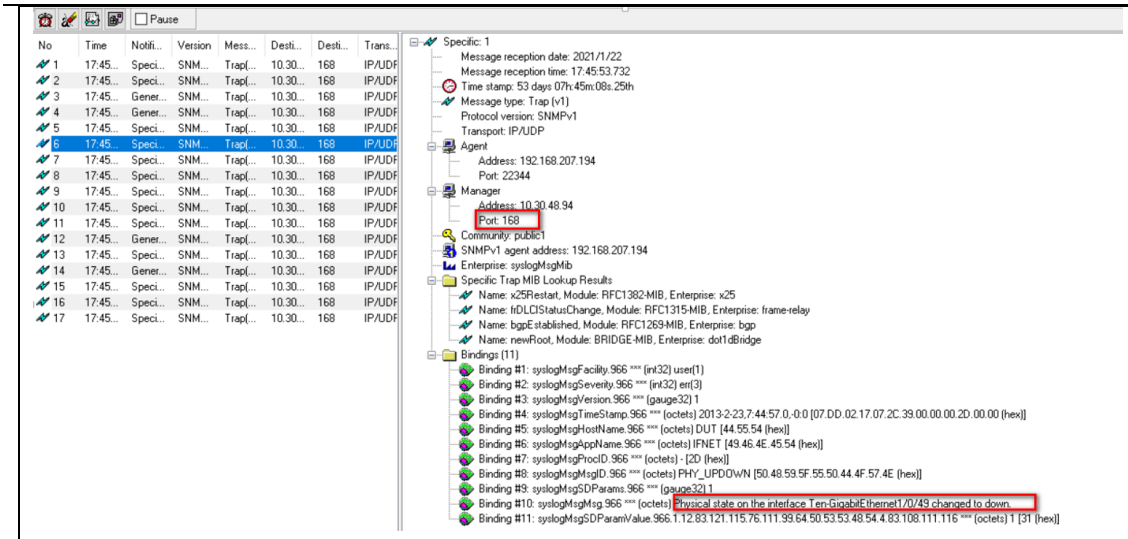
5. Simulate to generate Trap event, result 1 is expected.


File Edit View SNMP Action Tools Window Help
Query MIB Ping
MIB Browser Preferences
General
Transport
MIB
Query Results
Colors
Formatting
Set
Info
Discovery
Table View
Edit
Agent Compare
Trace
Windows
Trap Ringer
Ports
SNMPv3
Notification Port Preferences
Registered notification ports
Port Transport Status
162 (Default) IP/UDP Down
162 (Default) IPv6/UDP Transport Not Installed
36880 (Default) IPX Transport Not Installed
Add...
Edit...
Delete
Select SNMP Agent Port And Tran...
Port 168
Transport IP/UDP
OK
Cancel
Default
OK
Cancel



Remote address: 192.168.207.194 port: 161 transport: IP/UDP
Local address: 192.168.207.17 port: 62261 transport: IP/UDP
Protocol version: SNMPv1
1: sysUpTimeInstance (timeticks) 53 days 01h:01m:14s.41th (458287441)

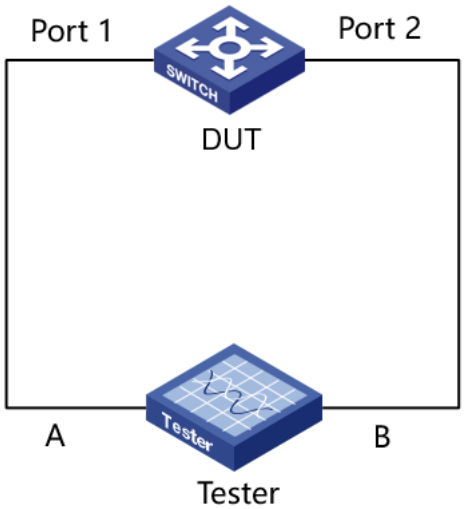
6. Shutdown a port , result 1 is expected.



☐ Passed	☐ Failed

5 QACL

5.1 L2 ACL

Test Item Name: Layer 2 ACL
Work Hour：20 min
Test Topology: 
Test Process: 1. Configure MAC ACL.

2. Send packets with source mac-address 0001-0001-0001 to Port 1 of DUT 1. Result 1 is expected.
3. Apply inbound packet-filter to Port 1. Result 2 is expected.
4. Clear the configuration on the Port 1.
5. Apply outbreak packet-filter to Port 2. Result 2 is expected.

Expect Results:

1. Port 2 can receive the traffic
2. Port 2 can't receive the traffic

Actual Result:

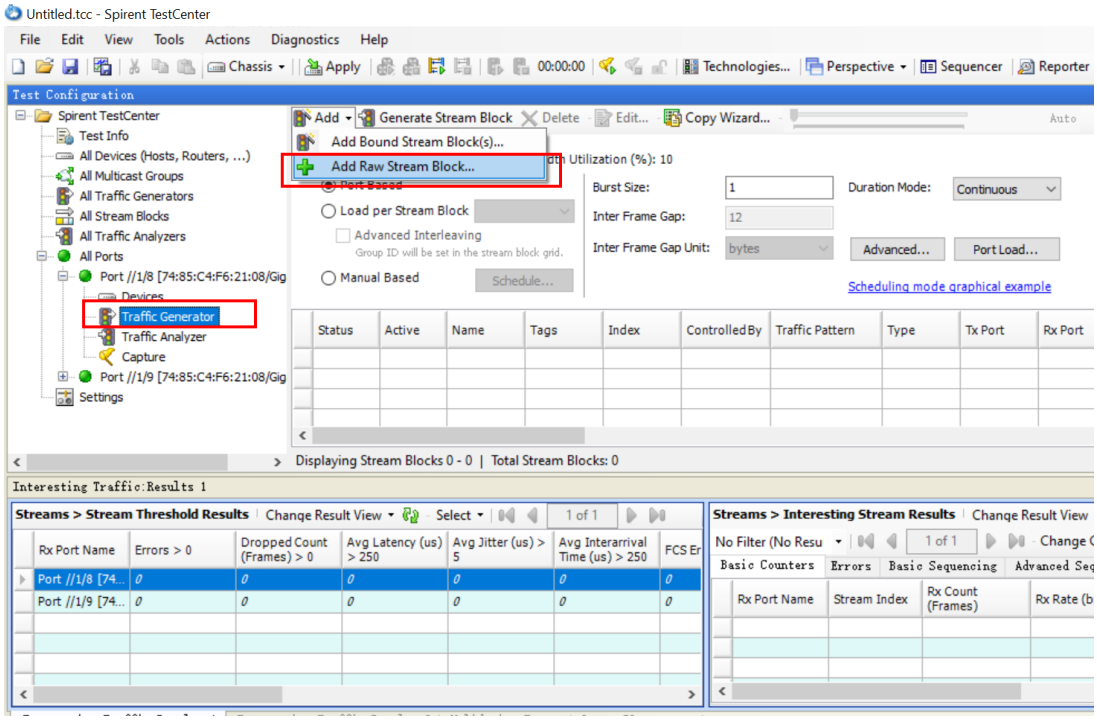
Configuration on DUT:

1. Configure MAC ACL. Deny the packets with the source MAC address 0001-0001-0001

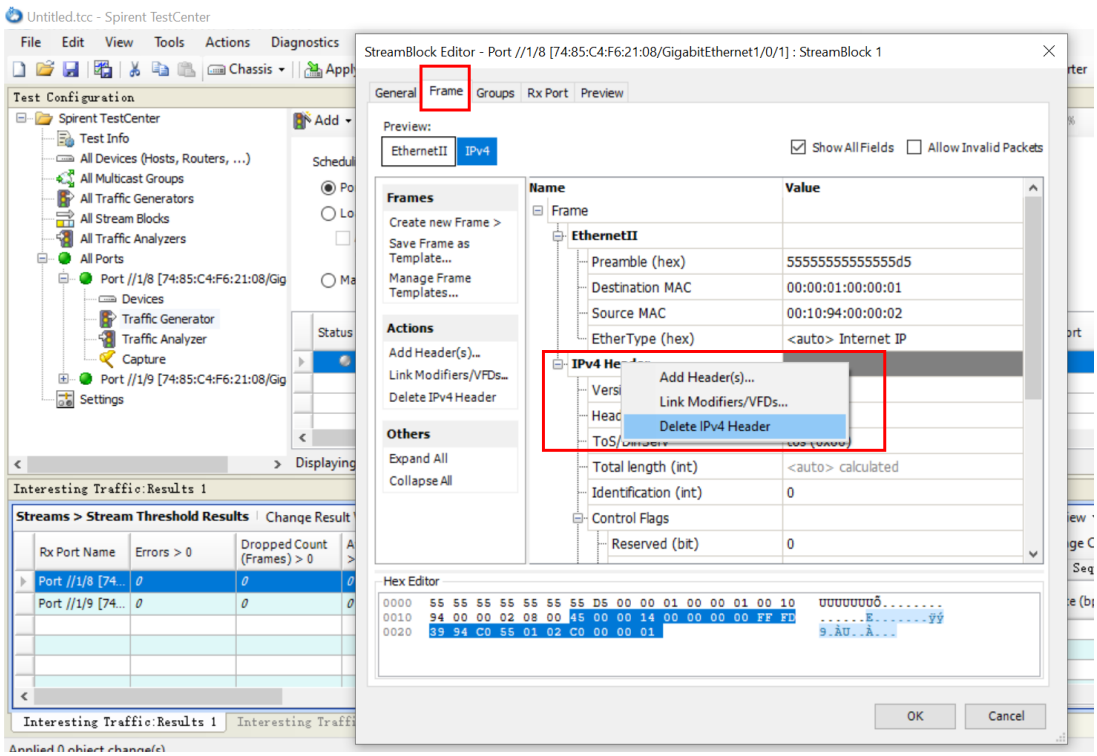
```
[DUT]acl number 4000
[DUT-acl-mac-4000]rule 0 deny source-mac 0001-0001-0001 ffff-ffff-ffff
```

2. Send packets with source mac-address 0001-0001-0001 to Port 1 of DUT. Result 1 is expected.

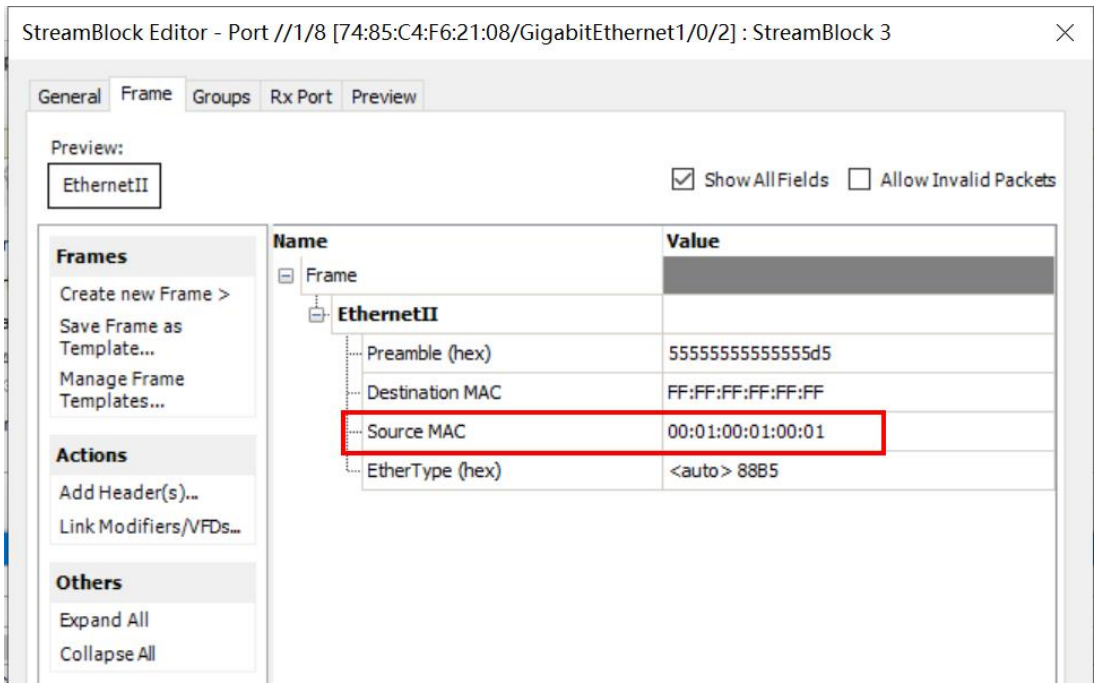
Add raw stream



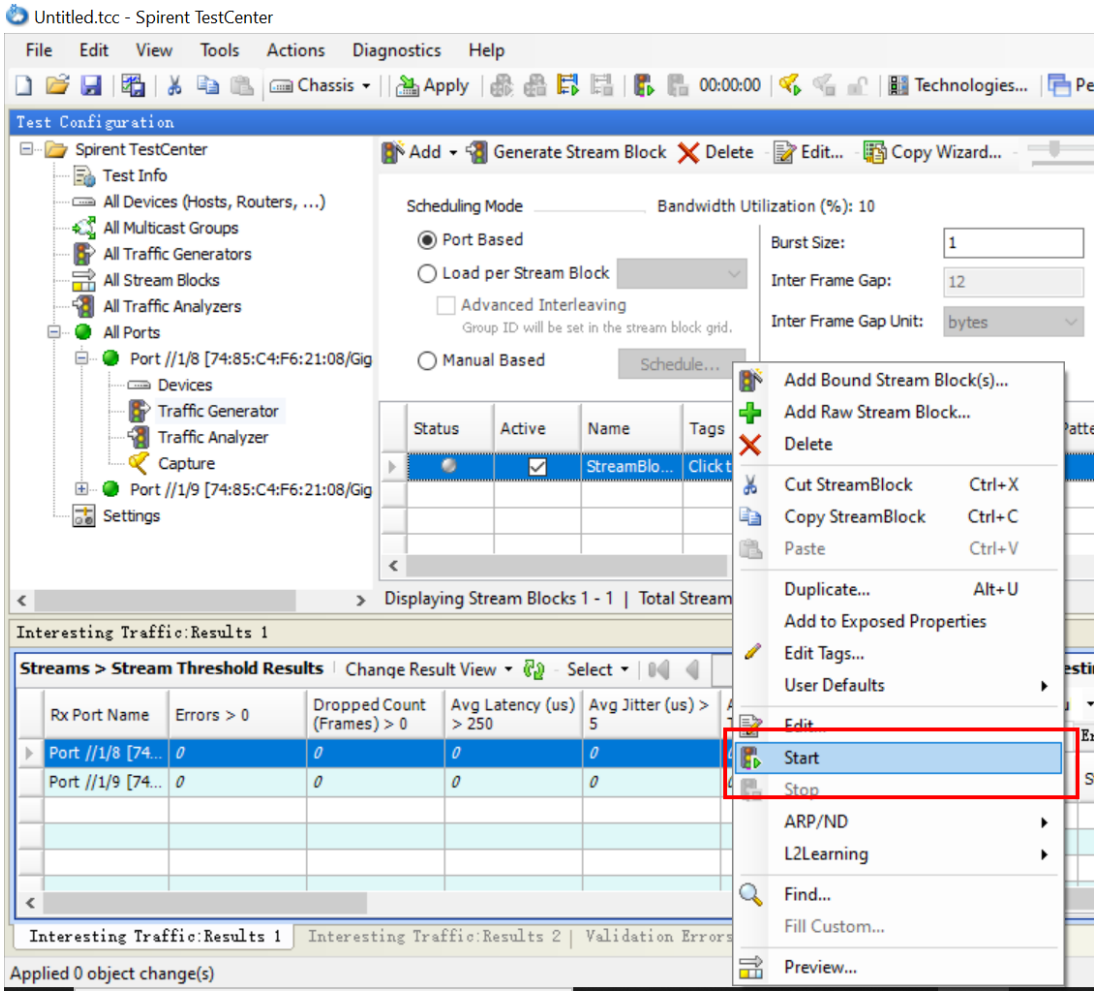
Delete the IPv4 header.



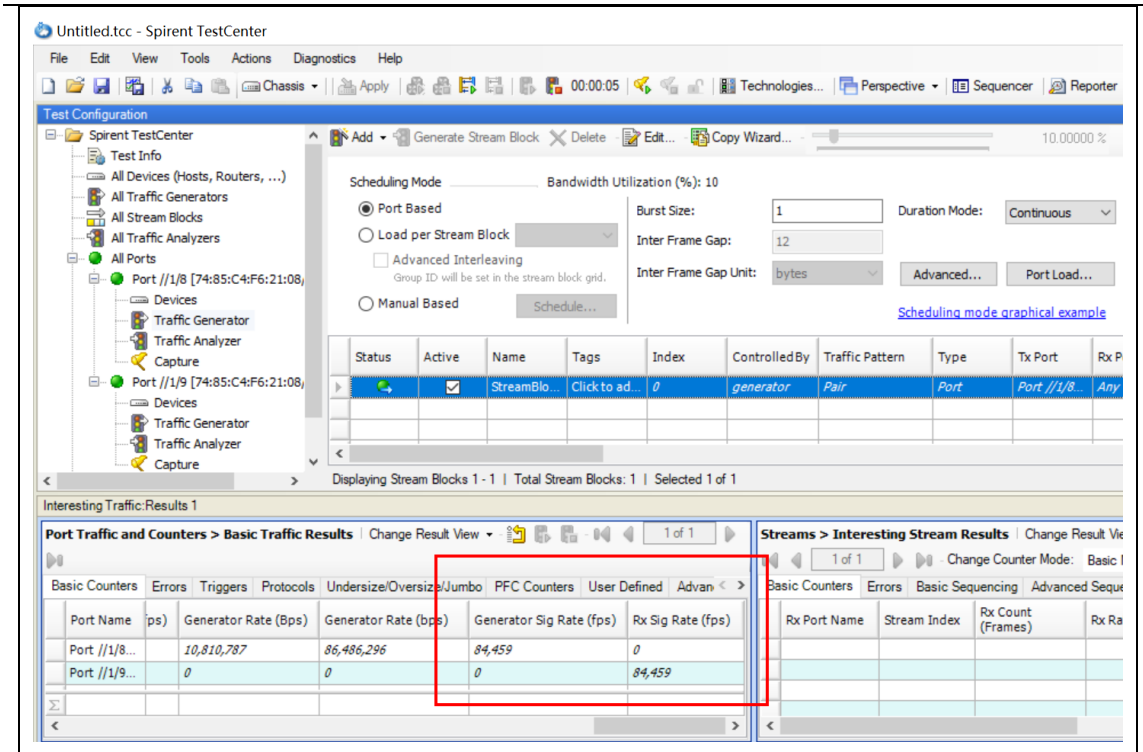
Change the source MAC to 0001-0001-0001



Start the traffic



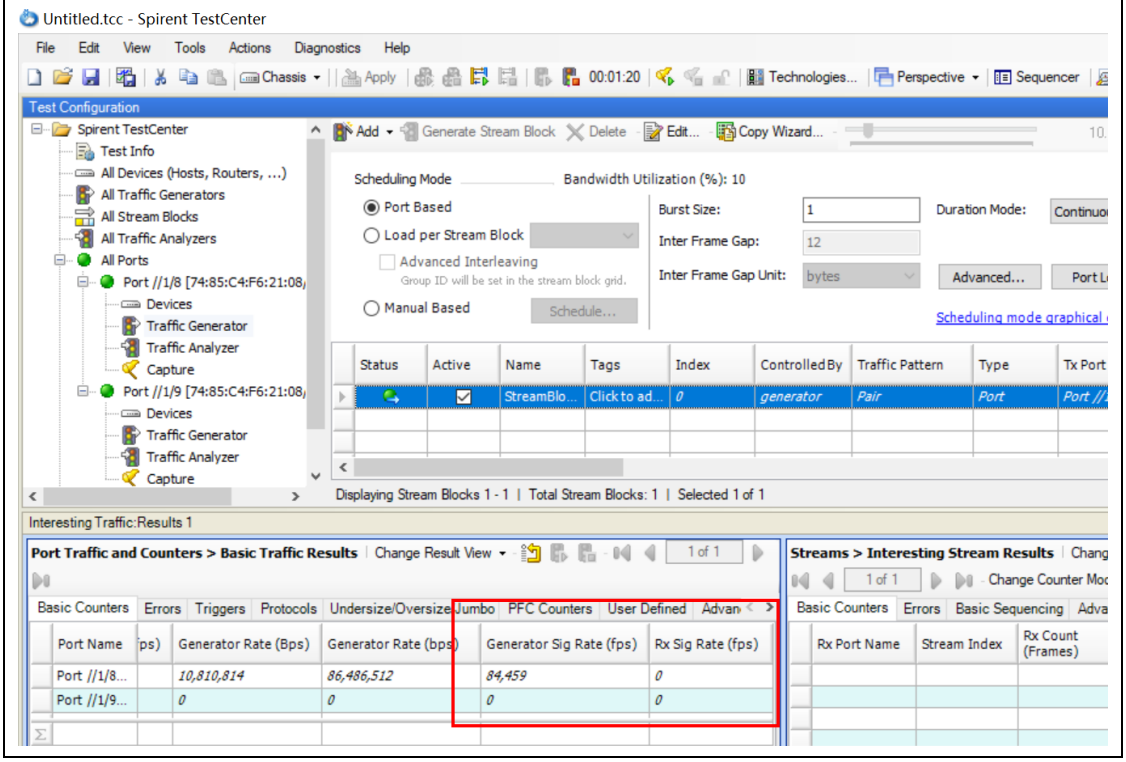
Port 2 can receive the traffic



3. Apply inbound packet-filter to Port 1. Result 2 is expected.

```
[DUT]interface GigabitEthernet 1/0/1
[DUT-GigabitEthernet1/0/1]packet-filter mac 4000 inbound
```

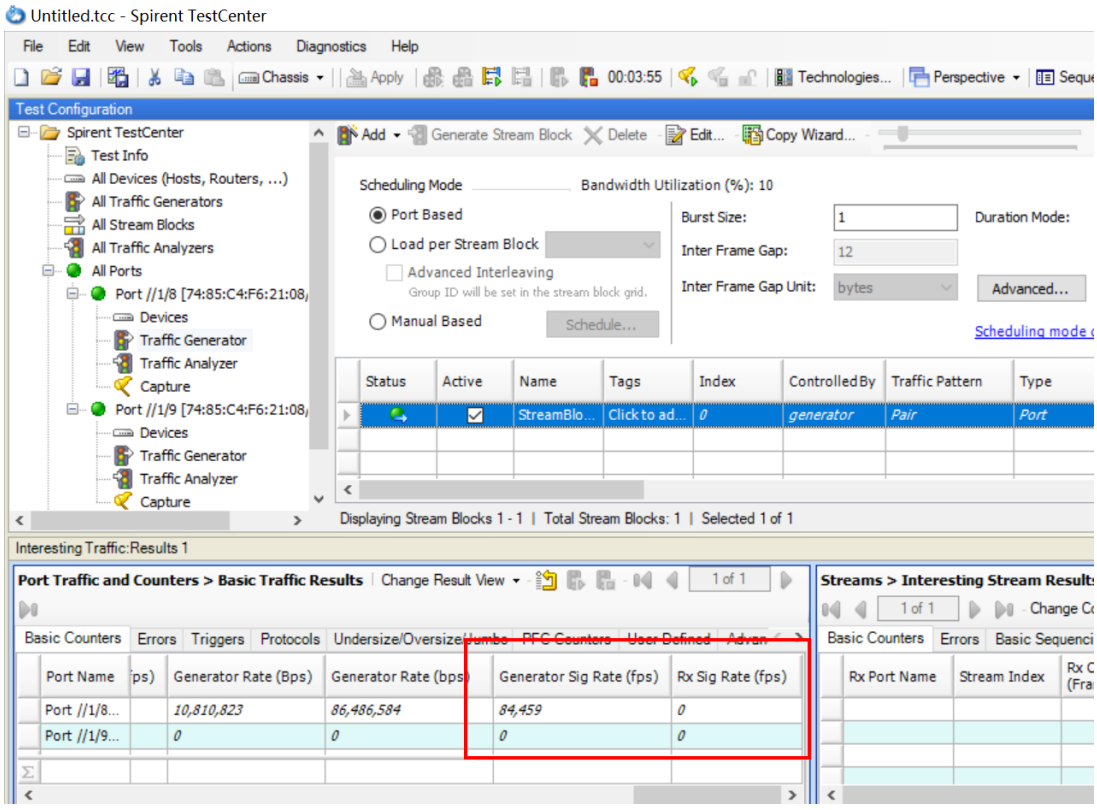
Port 2 can’t receive the traffic



4. Clear the configuration on the Port 1 .Apply outbreak packet-filter to Port 2. Result 2 is expected.

```
[DUT-GigabitEthernet1/0/1]undo packet-filter mac 4000 inbound
[DUT-GigabitEthernet1/0/1]interface GigabitEthernet 1/0/2
[DUT-GigabitEthernet1/0/2]packet-filter mac 4000 outbound
```

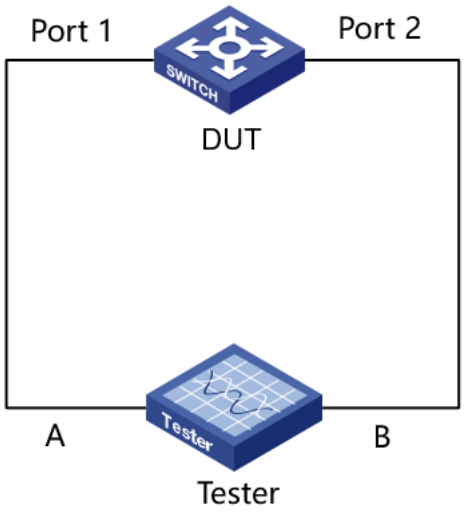
Port 2 can't receive the traffic



☐ Passed	☐ Failed

5.2 L3 ACL

Test Item Name: Layer 3 ACL
Work Hour：20 min
Test Topology:



Test Process:

1. Configure IPv4 ACL.
2. Send packets with source IP address 10.10.10.20 to Port 1 of DUT 1. Result 1 is expected.
3. Apply inbound packet-filter to Port 1. Result 2 is expected.
4. Clear the configuration on the Port 1.
5. Apply outbreak packet-filter to Port 2. Result 2 is expected.

Expect Results:

1. Port 2 can receive the traffic
2. Port 2 can't receive the traffic

Actual Result:

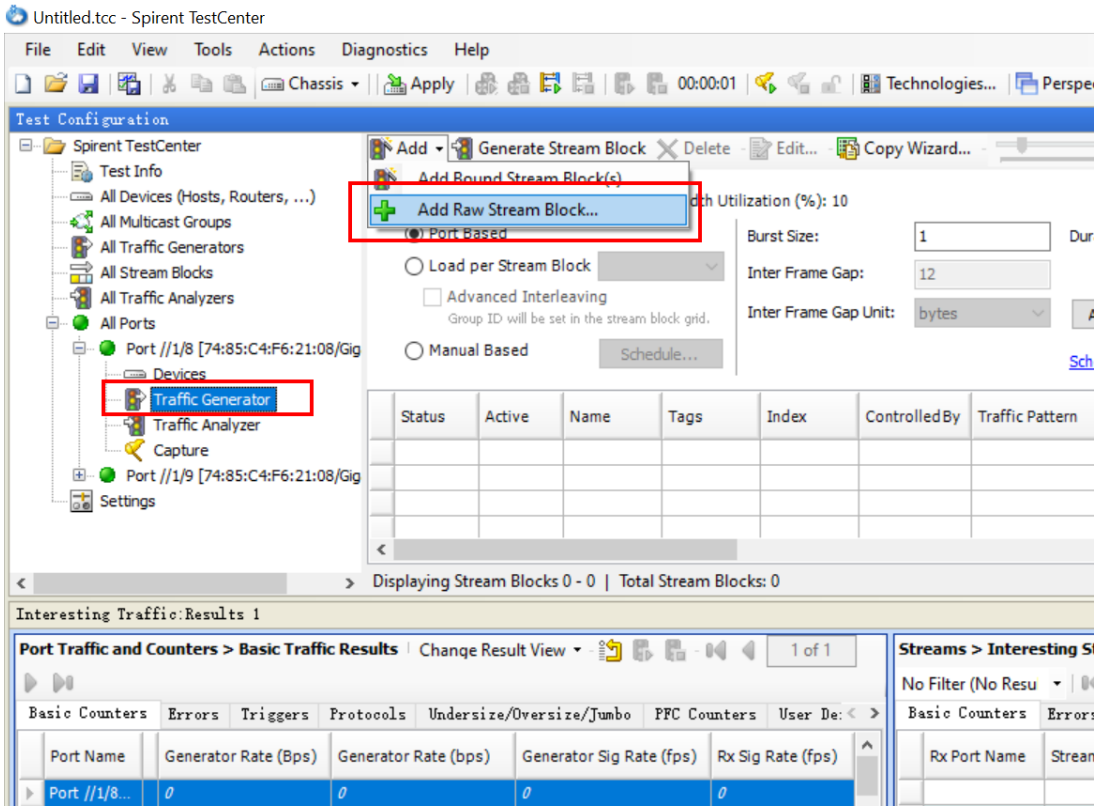
Configuration on DUT:

1. Configure IPv4 ACL.

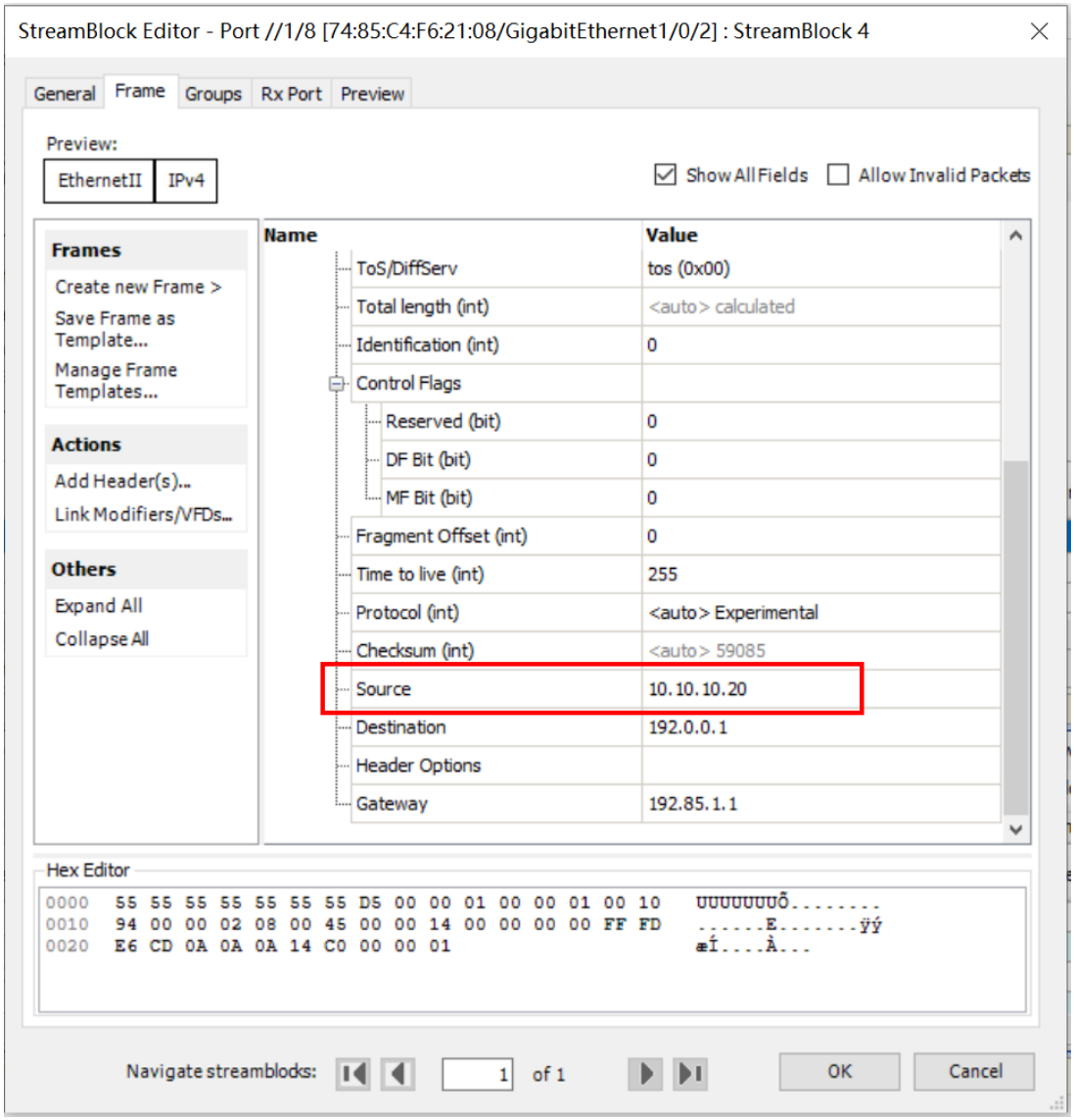
```
[DUT]acl number 2000
[DUT-acl-ipv4-basic-2000]rule 0 deny source 10.10.10.20 0
```

2. Send packets with source IP address 10.10.10.20 to Port 1 of DUT 1. Result 1 is expected.

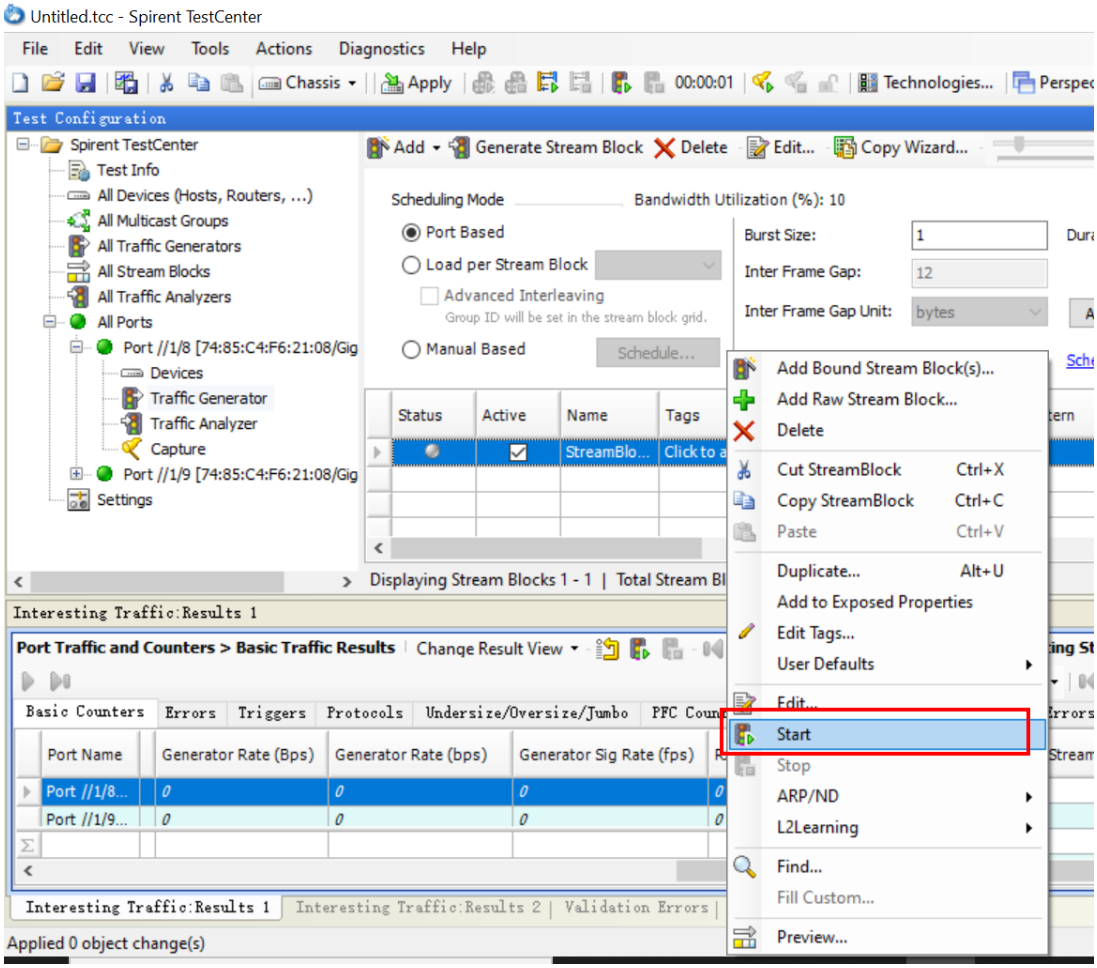
Add raw stream.



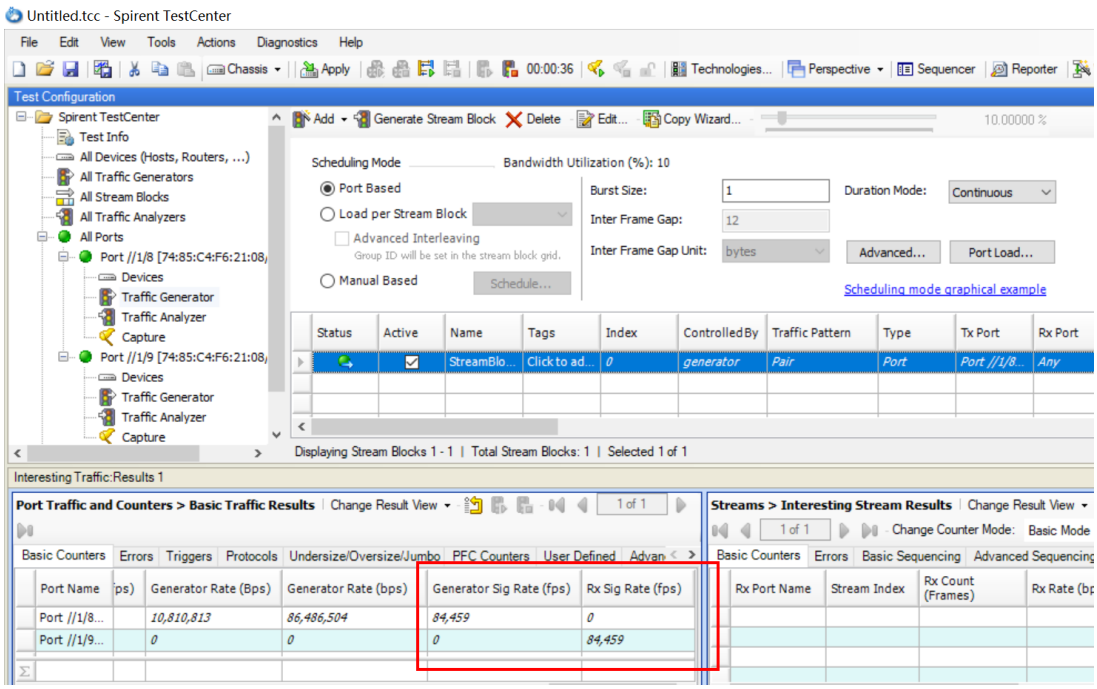
Change the source IP address to 10.10.10.20



Start the traffic



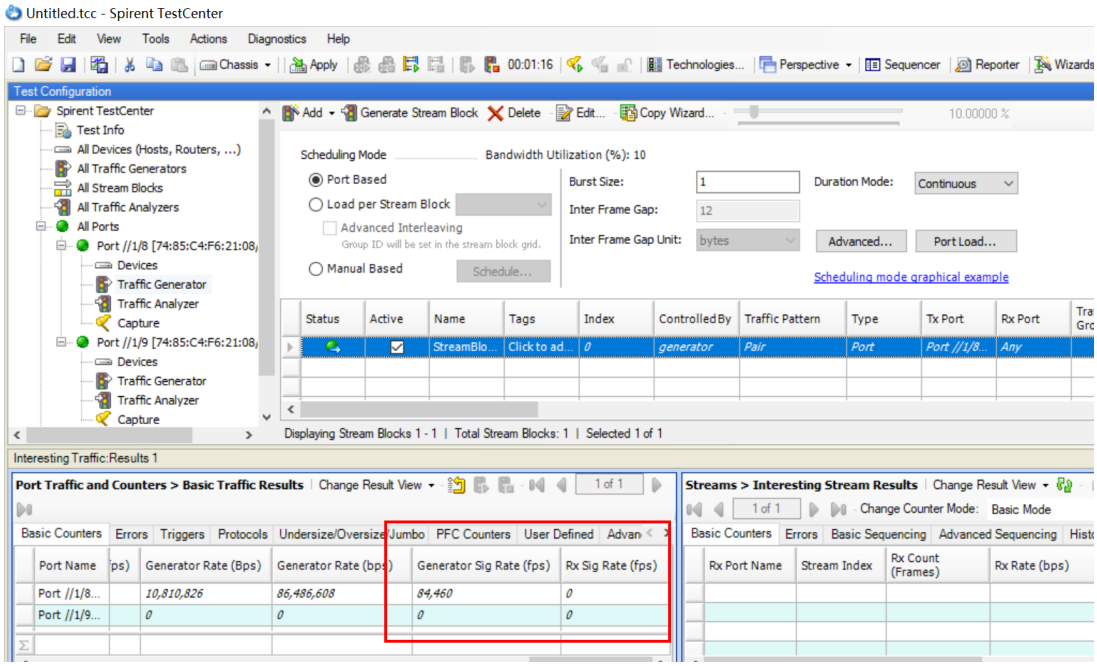
Port 2 can receive the traffic



3. Apply inbound packet-filter to Port 1. Result 2 is expected.

```
[DUT]int GigabitEthernet 1/0/1
[DUT-GigabitEthernet1/0/1]packet-filter 2000 inbound
```

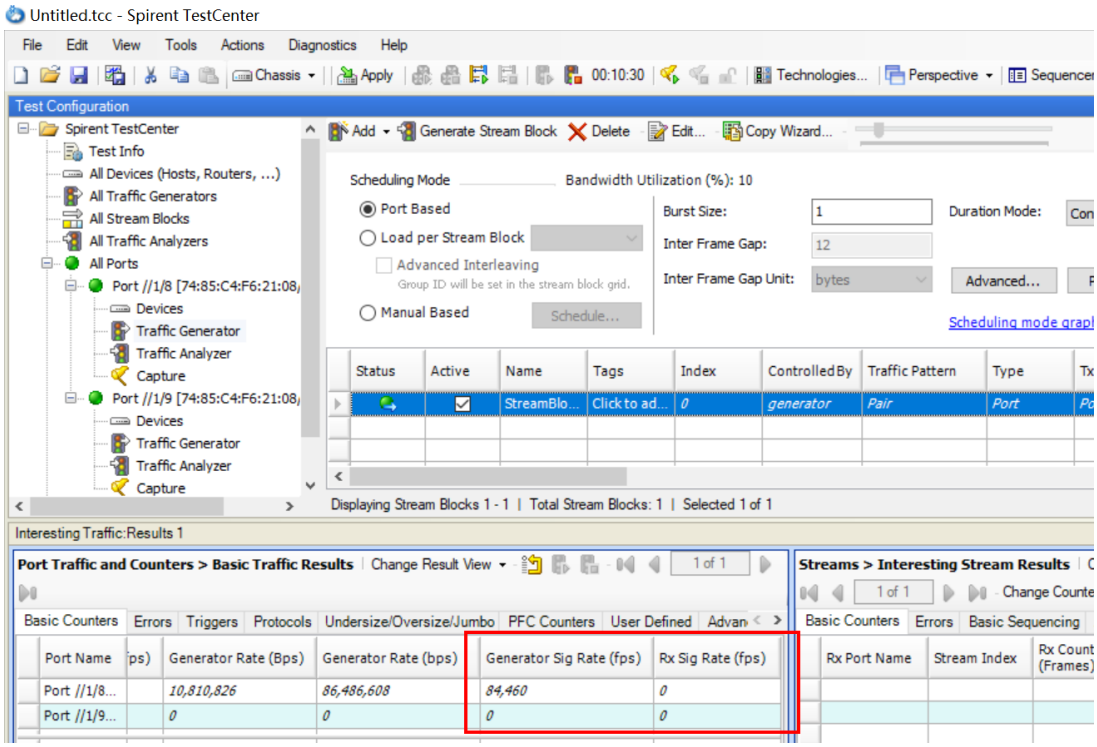
Port 2 can't receive the traffic



4. Clear the configuration on the Port 1. Apply outbreak packet-filter to Port 2. Result 2 is expected.

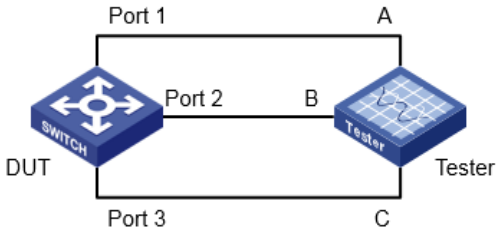
```
[DUT]interface GigabitEthernet 1/0/1
[DUT-GigabitEthernet1/0/1]undo packet-filter 2000 inbound
[DUT-GigabitEthernet1/0/1]interface GigabitEthernet 1/0/2
[DUT-GigabitEthernet1/0/2]packet-filter 2000 outbound
```

Port 2 can't receive the traffic



☐ Passed	☐ Failed

5.3 Traffic Classification

Test Item Name: Traffic Classification
Work Hour: 50 min
Test Topology: 
Test Process:

1. Configure traffic classifier to match the traffic with VLAN ID 100, configure traffic behavior to remark it to 200, and configure the corresponding QoS policy.
2. Configure Port 1/2 as trunk mode and permit VLAN 100 and 200 to pass.
3. Send packets with VLAN 100. Result 1 is expected.
4. Apply QoS policy to Port 1. Result 2 is expected.
5. Configure traffic classifier to match the traffic with COS 3, configure traffic behavior to remark it to 6, and configure the corresponding QoS policy.
6. Send packets with COS 3. Result 3 is expected.
7. Apply QoS policy to Port 1. Result 4 is expected.
8. Configure traffic classifier to match the traffic with DSCP 3, configure traffic behavior to remark it to 6, and configure the corresponding QoS policy.
9. Send packets with DSCP 3. Result 3 is expected.
10. Apply QoS policy to Port 1. Result 4 is expected.

Expect Results:

1. Port 2 can receive the traffic with VLAN tag 100.
2. Port 2 can receive the traffic with VLAN tag 200.
3. Port 2 can receive the traffic with COS 3.
4. Port 2 can receive the traffic with COS 6.
5. Port 2 can receive the traffic with DSCP 3.
6. Port 2 can receive the traffic with DSCP 6.

Actual Result：

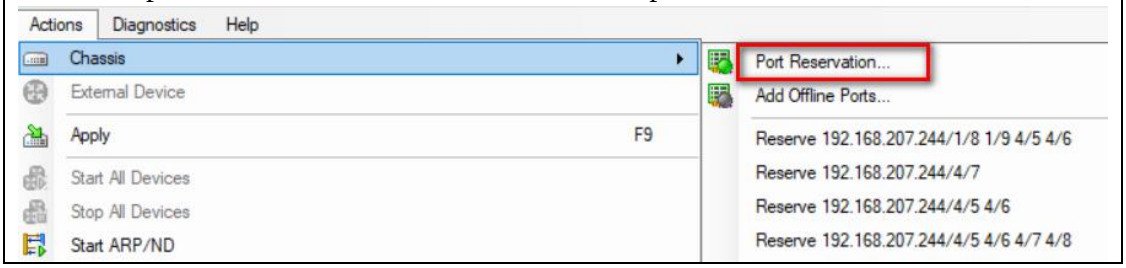
1. Configure traffic classifier to match the traffic with VLAN ID 100, configure traffic behavior to remark it to 200, and configure the corresponding QoS policy.

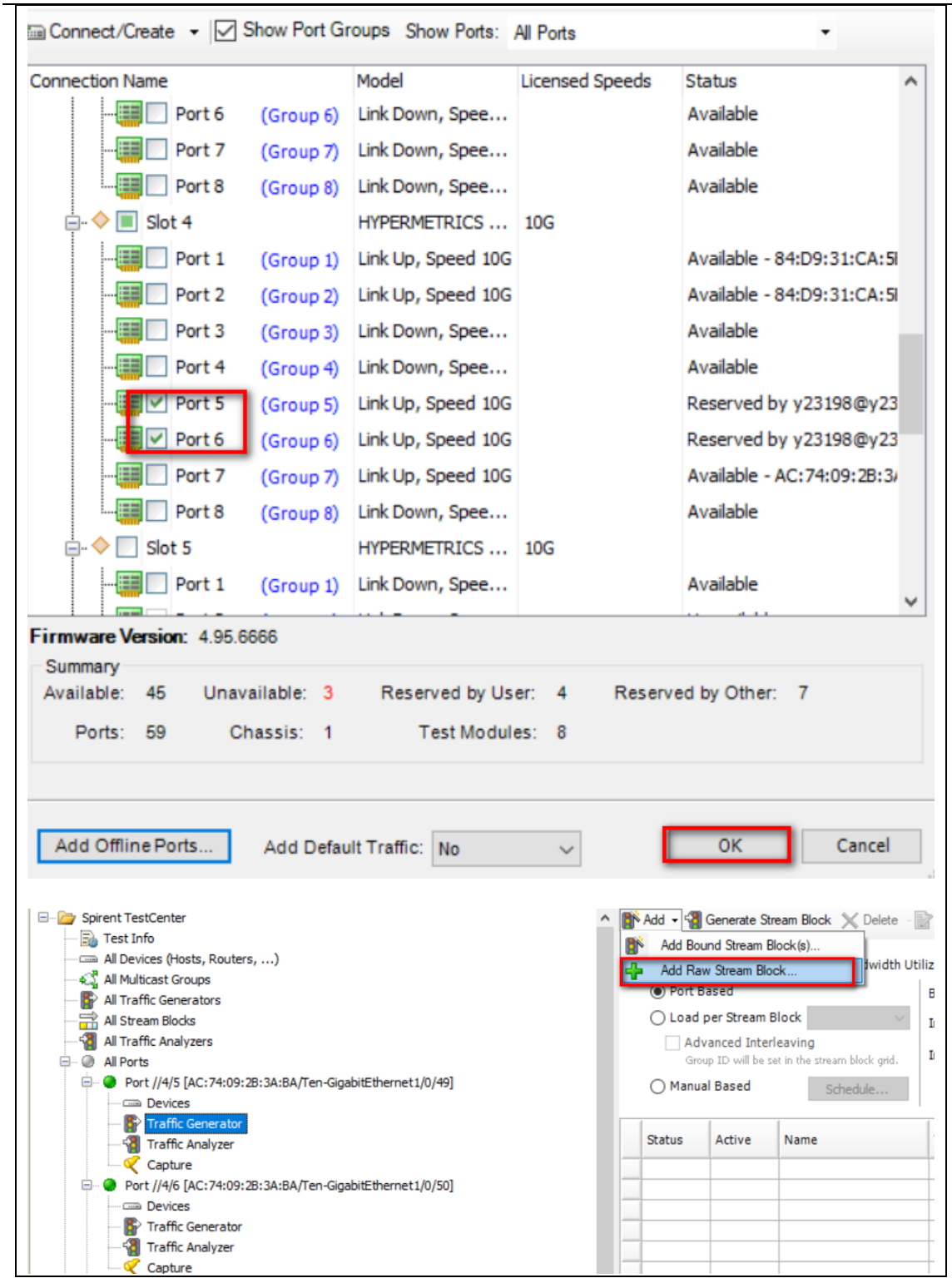
```
[DUT]traffic classifier 1
[DUT-classifier-1]display this
#
traffic classifier 1 operator and
 if-match service-vlan-id 100
#
[DUT]traffic behavior 1
[DUT-behavior-1]display this
#
traffic behavior 1
 remark service-vlan-id 200
#
```

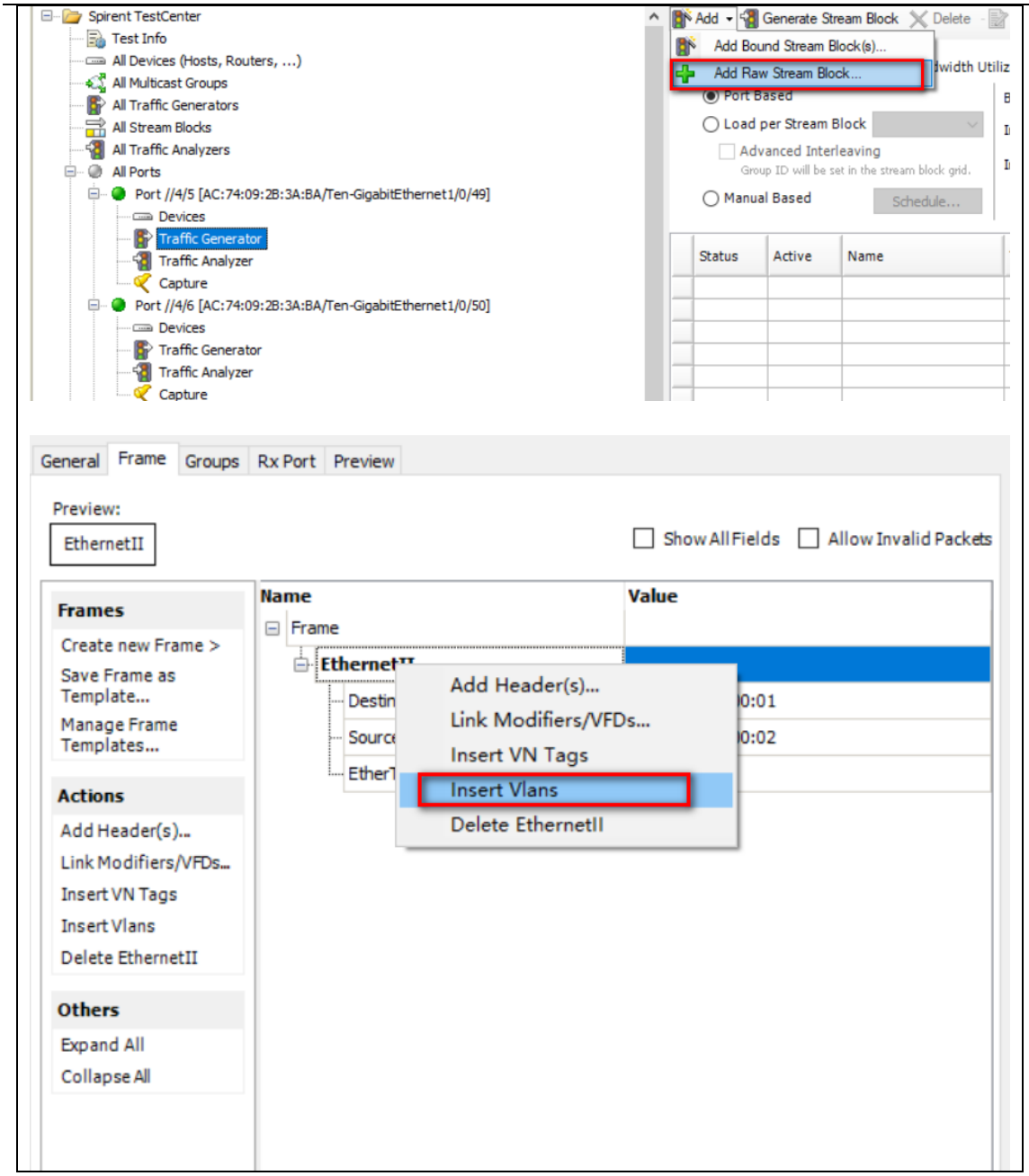
2. Configure Port 1/2 as trunk mode and permit VLAN 100 and 200 to pass.

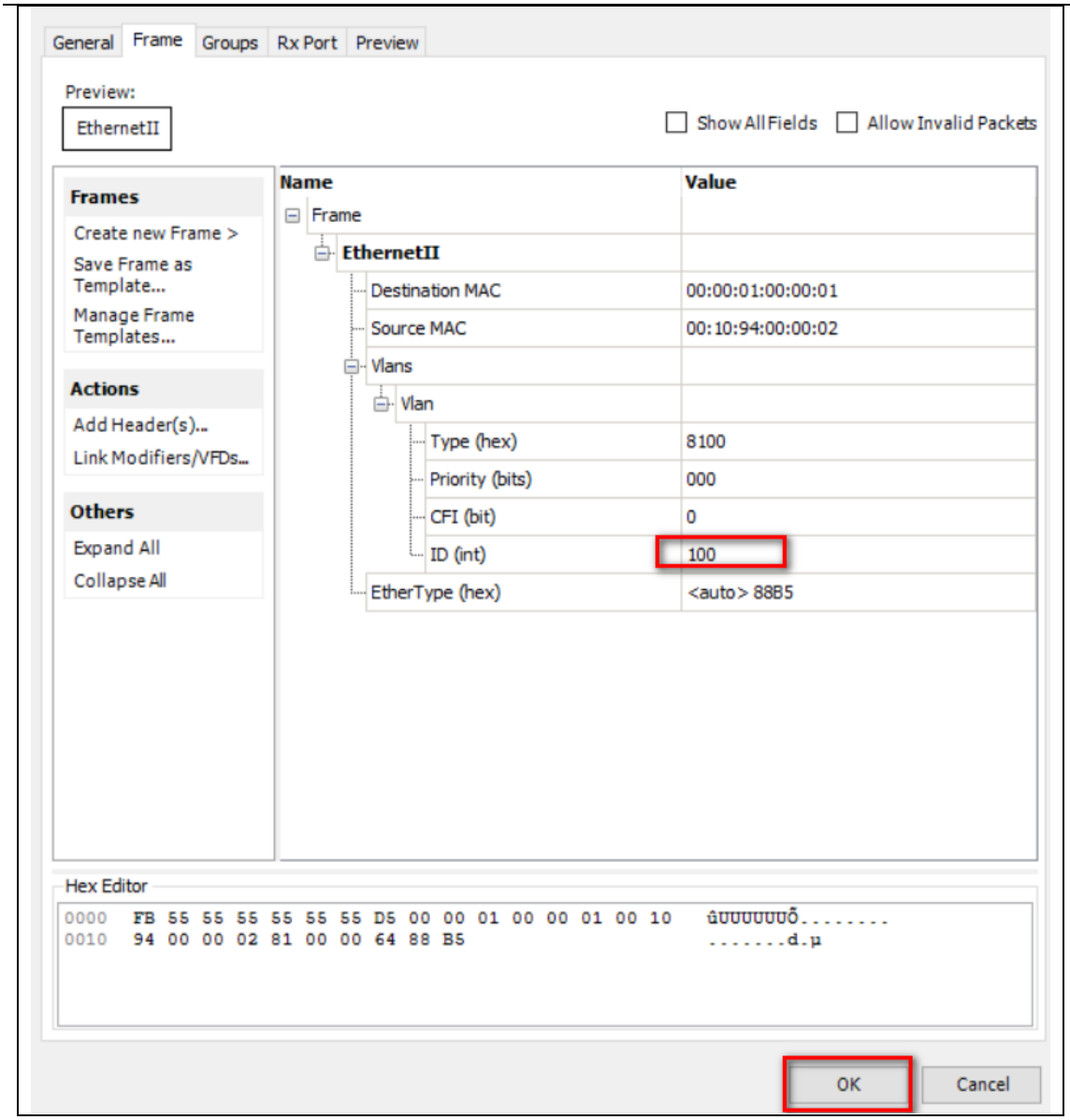
```
[DUT-Ten-GigabitEthernet1/0/49]display this
#
interface Ten-GigabitEthernet1/0/49
 port link-mode bridge
 port link-type trunk
 port trunk permit vlan 1 100 200
#
[DUT-Ten-GigabitEthernet1/0/50]display this
#
interface Ten-GigabitEthernet1/0/50
 port link-mode bridge
 port link-type trunk
 port trunk permit vlan 1 100 200
#
```

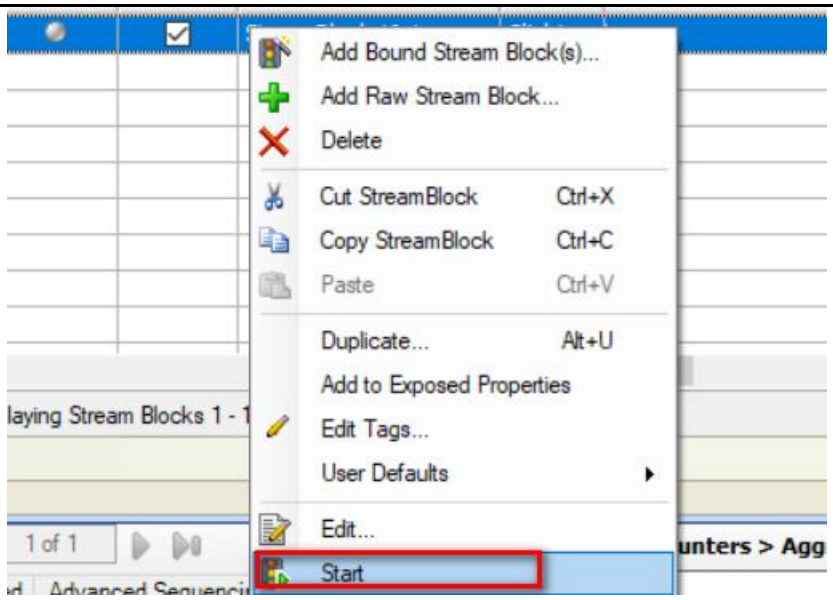
3. Send packets with VLAN 100. Result 1 is expected.





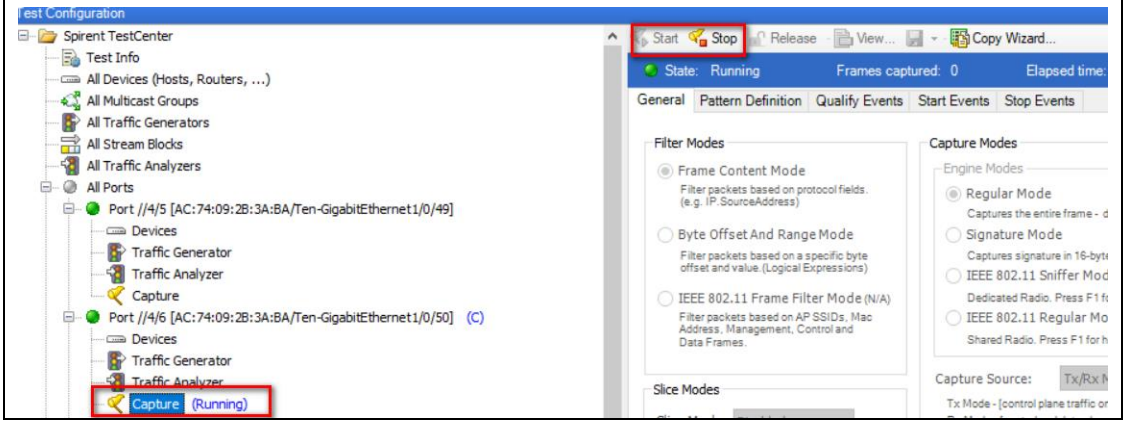

Spirent TestCenter
Test Info
All Devices (Hosts, Routers, ...)
All Multicast Groups
All Traffic Generators
All Stream Blocks
All Traffic Analyzers
All Ports
Port //4/5 [AC:74:09:2B:3A:BA/Ten-GigabitEthernet1/0/49]
Devices
Traffic Generator
Traffic Analyzer
Capture
Port //4/6 [AC:74:09:2B:3A:BA/Ten-GigabitEthernet1/0/50]
Devices
Traffic Generator
Traffic Analyzer
Capture
Add
Generate Stream Block
Delete
Add Bound Stream Block(s)...
Add Raw Stream Block...
Port Based
Load per Stream Block
Advanced Interleaving
Group ID will be set in the stream block grid.
Manual Based
Schedule...
Status
Active
Name
General
Frame
Groups
Rx Port
Preview
Preview:
EthernetII
Show All Fields
Allow Invalid Packets
Frames
Create new Frame >
Save Frame as Template...
Manage Frame Templates...
Actions
Add Header(s)...
Link Modifiers/VFDs...
Insert VN Tags
Insert Vlans
Delete EthernetII
Others
Expand All
Collapse All
Name
Value
Frame
Add Header(s)...
Link Modifiers/VFDs...
Insert VN Tags
Insert Vlans
Delete EthernetII

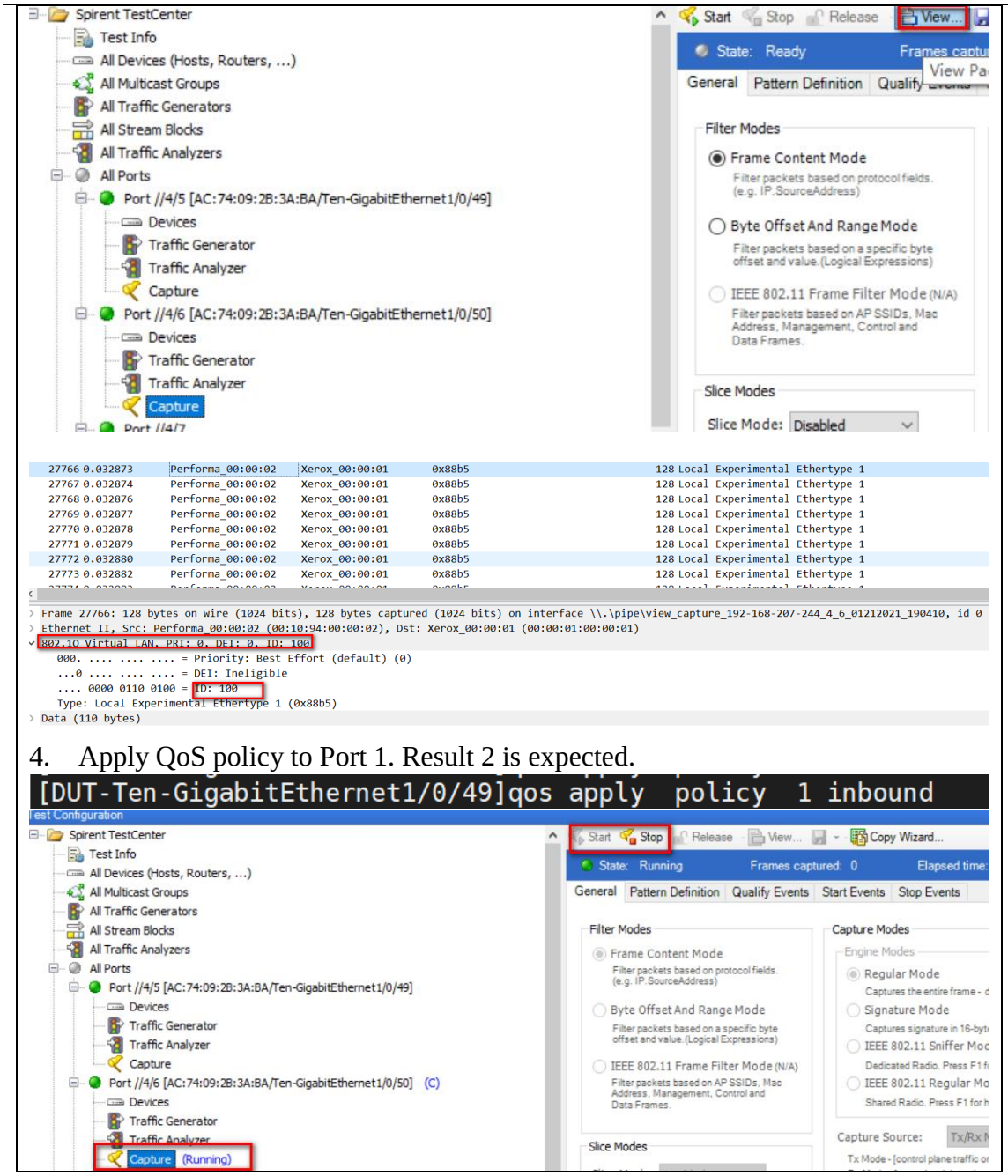




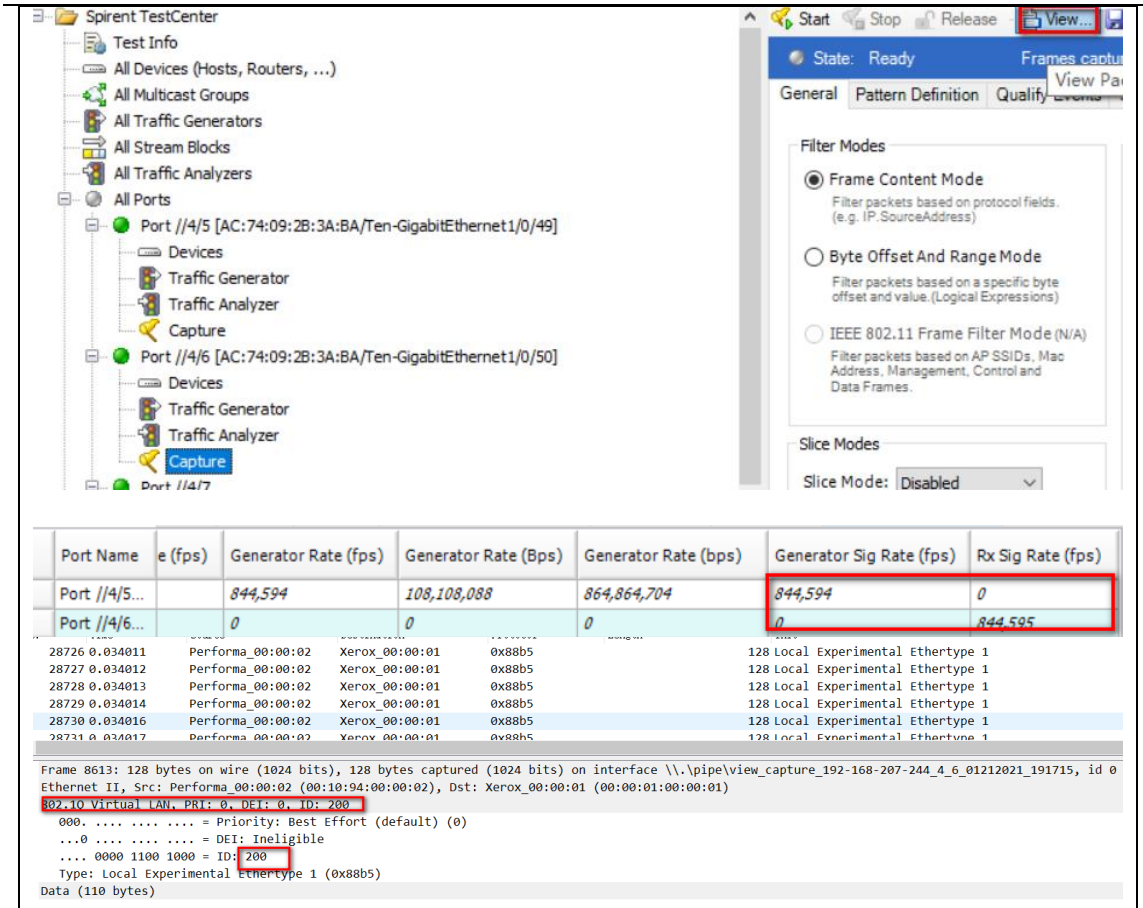
Port Name	e (fps)	Generator Rate (fps)	Generator Rate (Bps)	Generator Rate (bps)	Generator Sig Rate (fps)	Rx Sig Rate (fps)
Port //4/5...		844,594	108,108,088	864,864,704	844,594	0
Port //4/6...		0	0	0	0	844,595

Note: when capturing, click start and after several seconds click stop, then choose view.





4. Apply QoS policy to Port 1. Result 2 is expected.

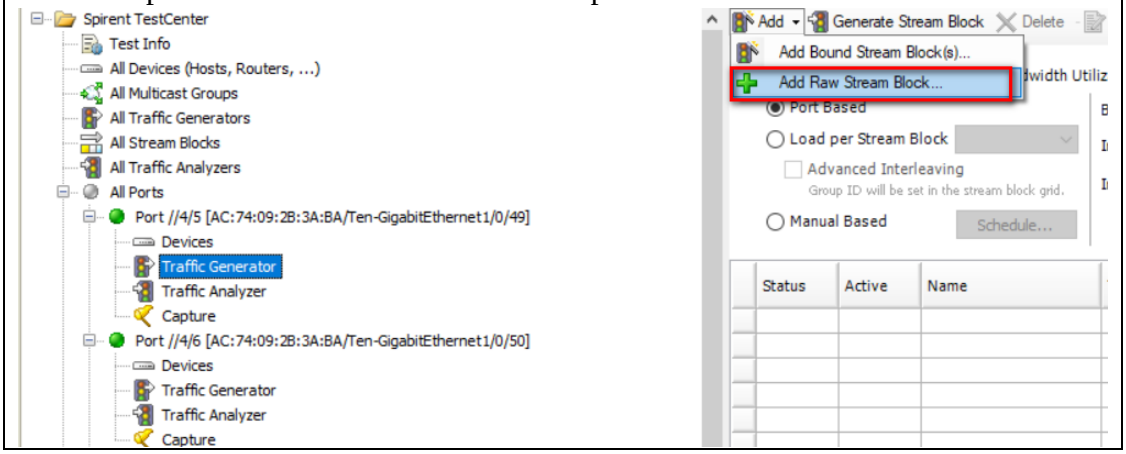


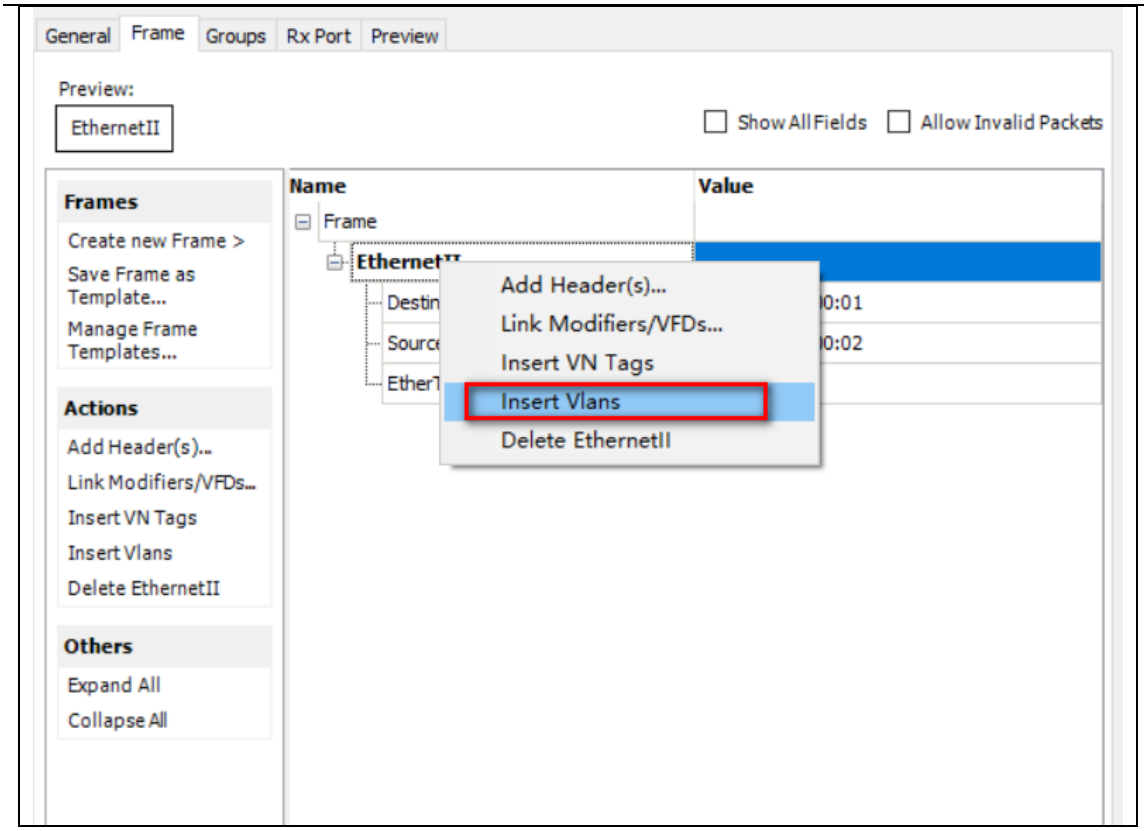
5. Configure traffic classifier to match the traffic with COS 3, configure traffic behavior to remark it to 6, and configure the corresponding QoS policy.

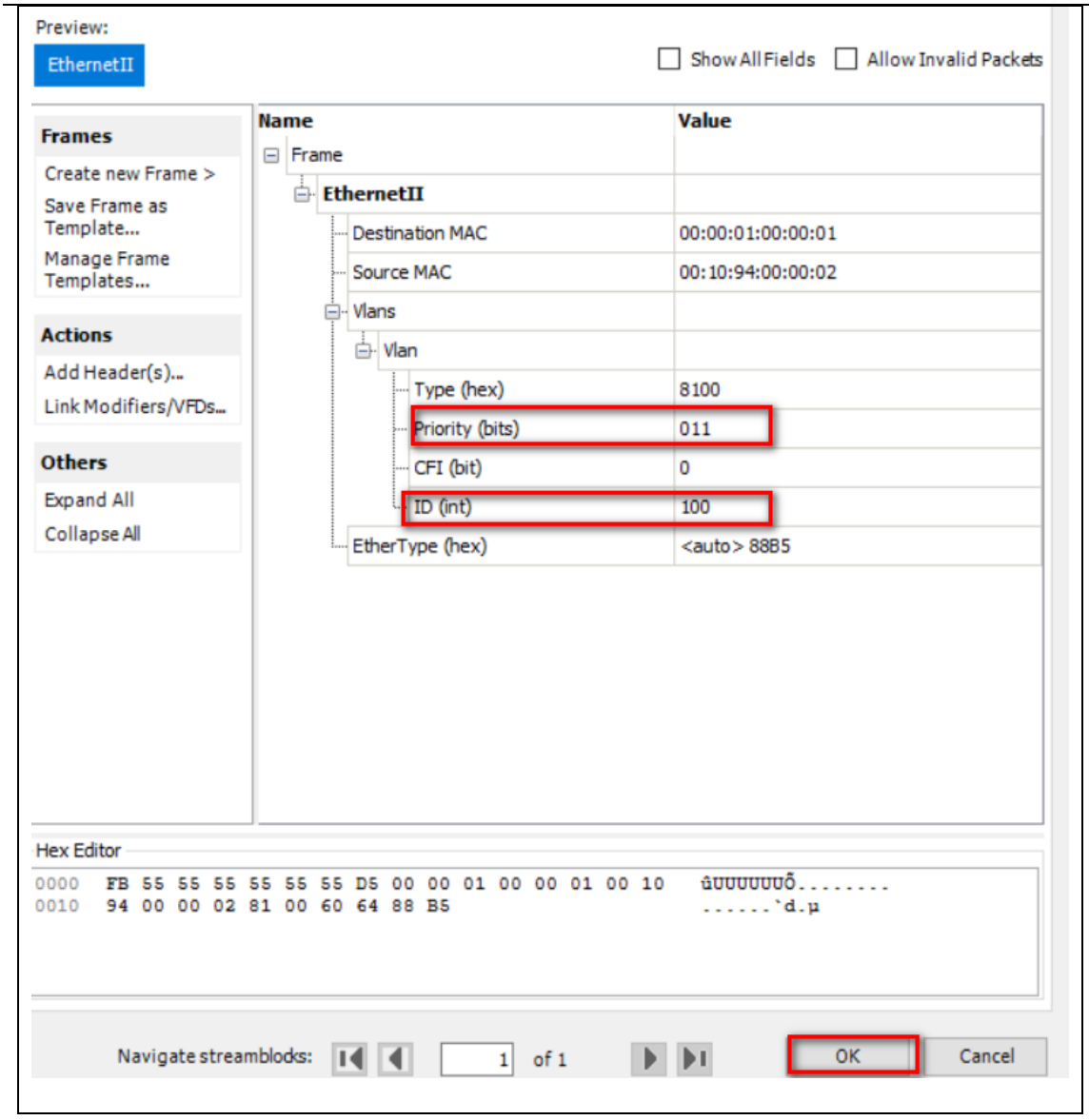
```
[DUT]vlan 100
[DUT-vlan100]interface Ten-GigabitEthernet 1/0/49
[DUT-Ten-GigabitEthernet1/0/49]display this
#
interface Ten-GigabitEthernet1/0/49
 port link-mode bridge
 port link-type trunk
 port trunk permit vlan 1 100
 qos trust dot1p
#
return
[DUT-Ten-GigabitEthernet1/0/49]interface Ten-GigabitEthernet 1/0/50
[DUT-Ten-GigabitEthernet1/0/50]display this
#
interface Ten-GigabitEthernet1/0/50
 port link-mode bridge
 port link-type trunk
 port trunk permit vlan 1 100
 qos trust dot1p
#
```

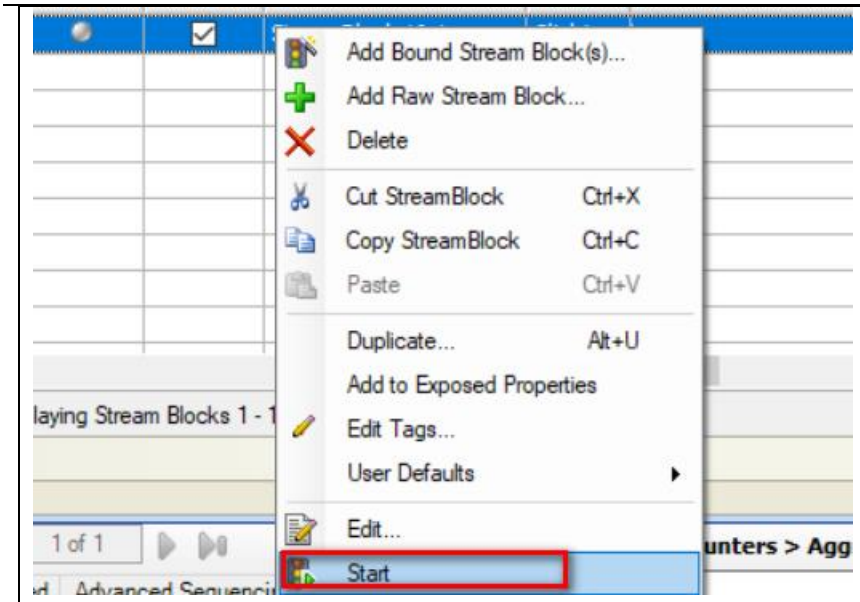
```
[DUT]traffic classifier 2
[DUT-classifier-2]display this
#
traffic classifier 2 operator and
 if-match service-dot1p 3
#
return
[DUT-classifier-2]traffic behavior 2
[DUT-behavior-2]display this
#
traffic behavior 2
 remark dot1p 6
#
return
[DUT-behavior-2]qos policy 2
[DUT-qospolicy-2]display this
#
qos policy 2
 classifier 2 behavior 2
#
return
```

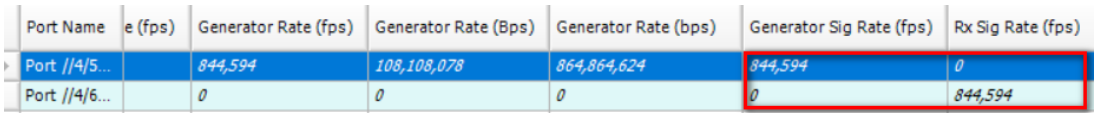
6. Send packets with COS 3. Result 3 is expected.

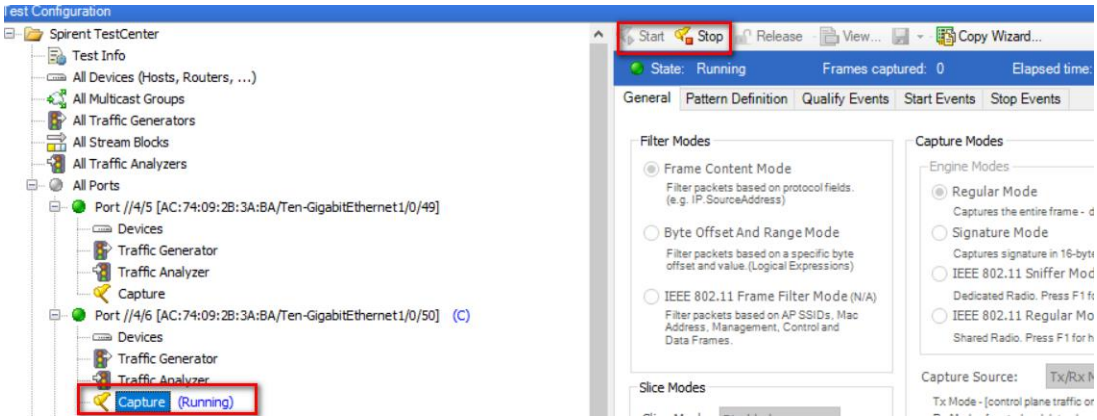


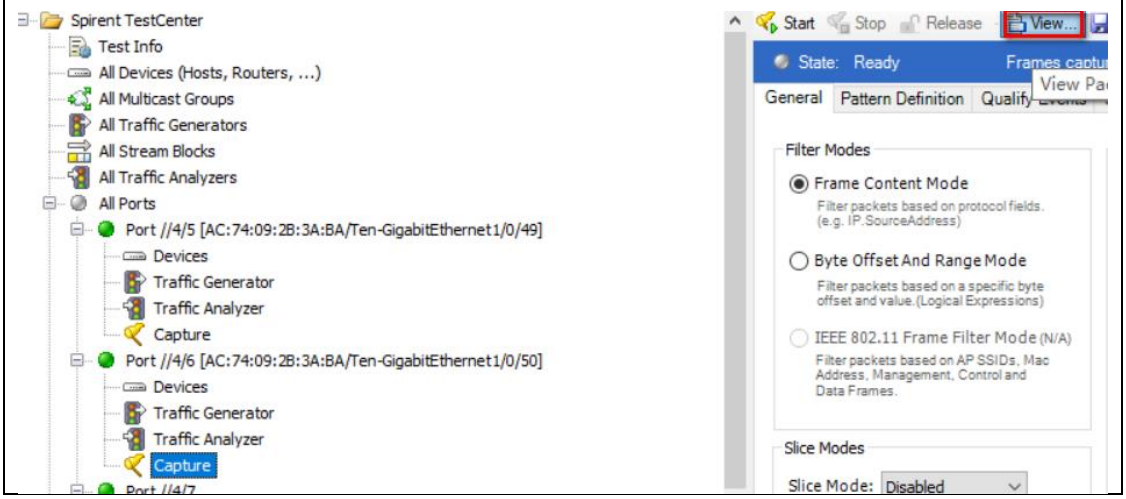

General
Frame
Groups
Rx Port
Preview
Preview:
EthernetII
Show All Fields
Allow Invalid Packets
Frames
Create new Frame >
Save Frame as Template...
Manage Frame Templates...
Actions
Add Header(s)...
Link Modifiers/VFDs...
Insert VN Tags
Insert Vlans
Delete EthernetII
Others
Expand All
Collapse All
Name
Value
Frame
Add Header(s)...
Link Modifiers/VFDs...
Insert VN Tags
Insert Vlans
Delete EthernetII









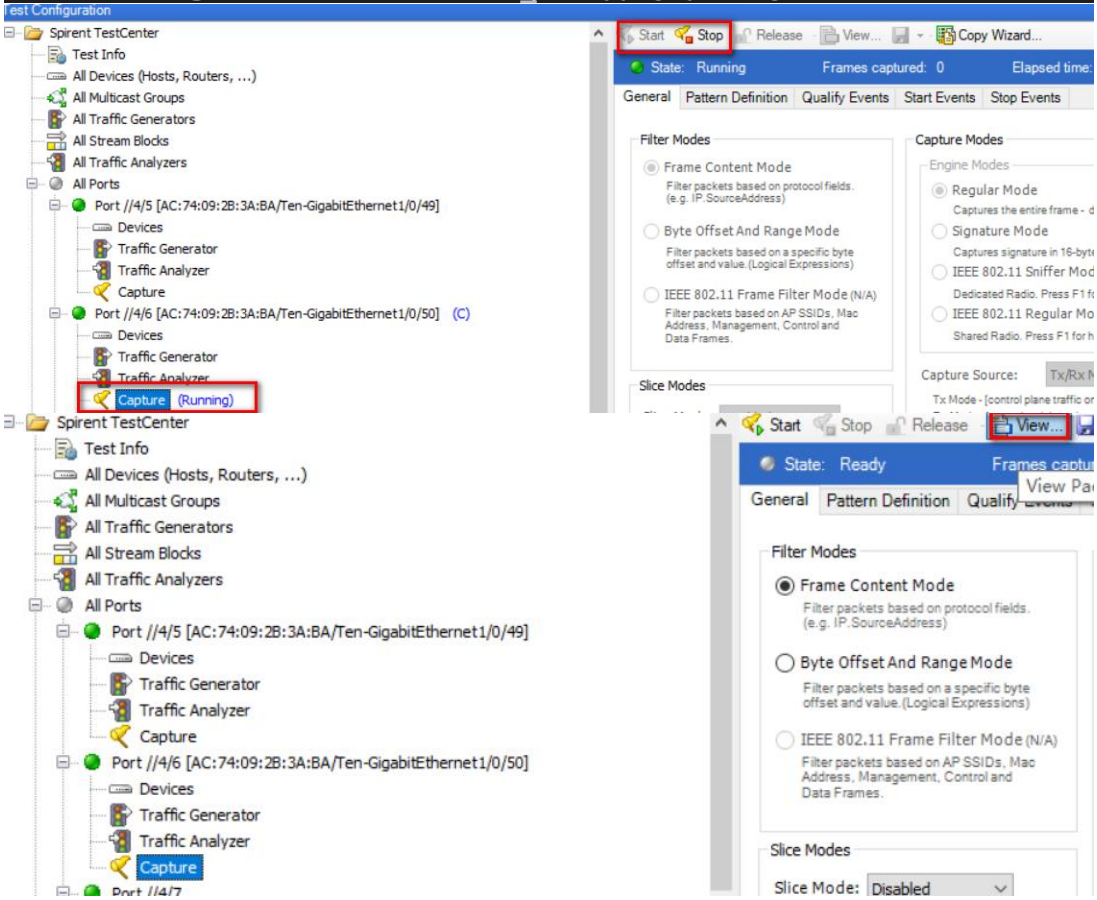


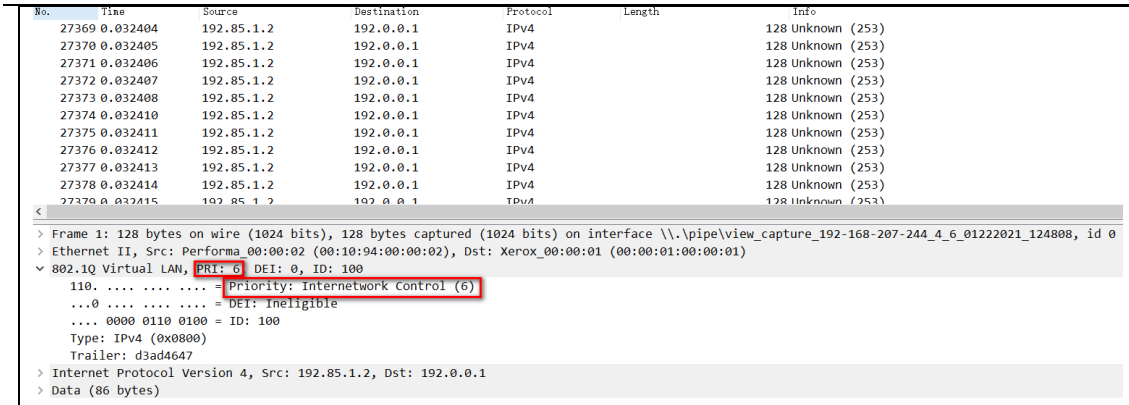
No.	Time	Source	Destination	Protocol	Length	Info
29991	0.035508	192.85.1.2	192.0.0.1	IPv4	128	Unknown (253)
29992	0.035509	192.85.1.2	192.0.0.1	IPv4	128	Unknown (253)
29993	0.035511	192.85.1.2	192.0.0.1	IPv4	128	Unknown (253)
29994	0.035512	192.85.1.2	192.0.0.1	IPv4	128	Unknown (253)
29995	0.035513	192.85.1.2	192.0.0.1	IPv4	128	Unknown (253)
29996	0.035514	192.85.1.2	192.0.0.1	IPv4	128	Unknown (253)
29997	0.035515	192.85.1.2	192.0.0.1	IPv4	128	Unknown (253)
29998	0.035517	192.85.1.2	192.0.0.1	IPv4	128	Unknown (253)
29999	0.035518	192.85.1.2	192.0.0.1	IPv4	128	Unknown (253)
30000	0.035519	192.85.1.2	192.0.0.1	IPv4	128	Unknown (253)
30001	0.035520	192.85.1.2	192.0.0.1	IPv4	128	Unknown (253)

```
> Frame 1: 128 bytes on wire (1024 bits), 128 bytes captured (1024 bits) on interface \\.\pipe\view_capture_192-168-207-244_4_6_01222021_124631, id 0
> Ethernet II, Src: Performa_00:00:02 (00:10:94:00:00:02), Dst: Xerox_00:00:01 (00:00:01:00:00:01)
v 802.1Q Virtual LAN, PRI: 3, DEI: 0, ID: 100
    011. .... .... .... = Priority: Critical Applications (3)
    ...0 .... .... .... = DEI: Ineligible
    .... 0000 0110 0100 = ID: 100
    Type: IPv4 (0x0800)
    Trailer: 686c5680
> Internet Protocol Version 4, Src: 192.85.1.2, Dst: 192.0.0.1
> Data (86 bytes)
```

7. Apply QoS policy to Port 1. Result 4 is expected.

```
[DUT-Ten-GigabitEthernet1/0/49]qos apply policy 2 inbound
```

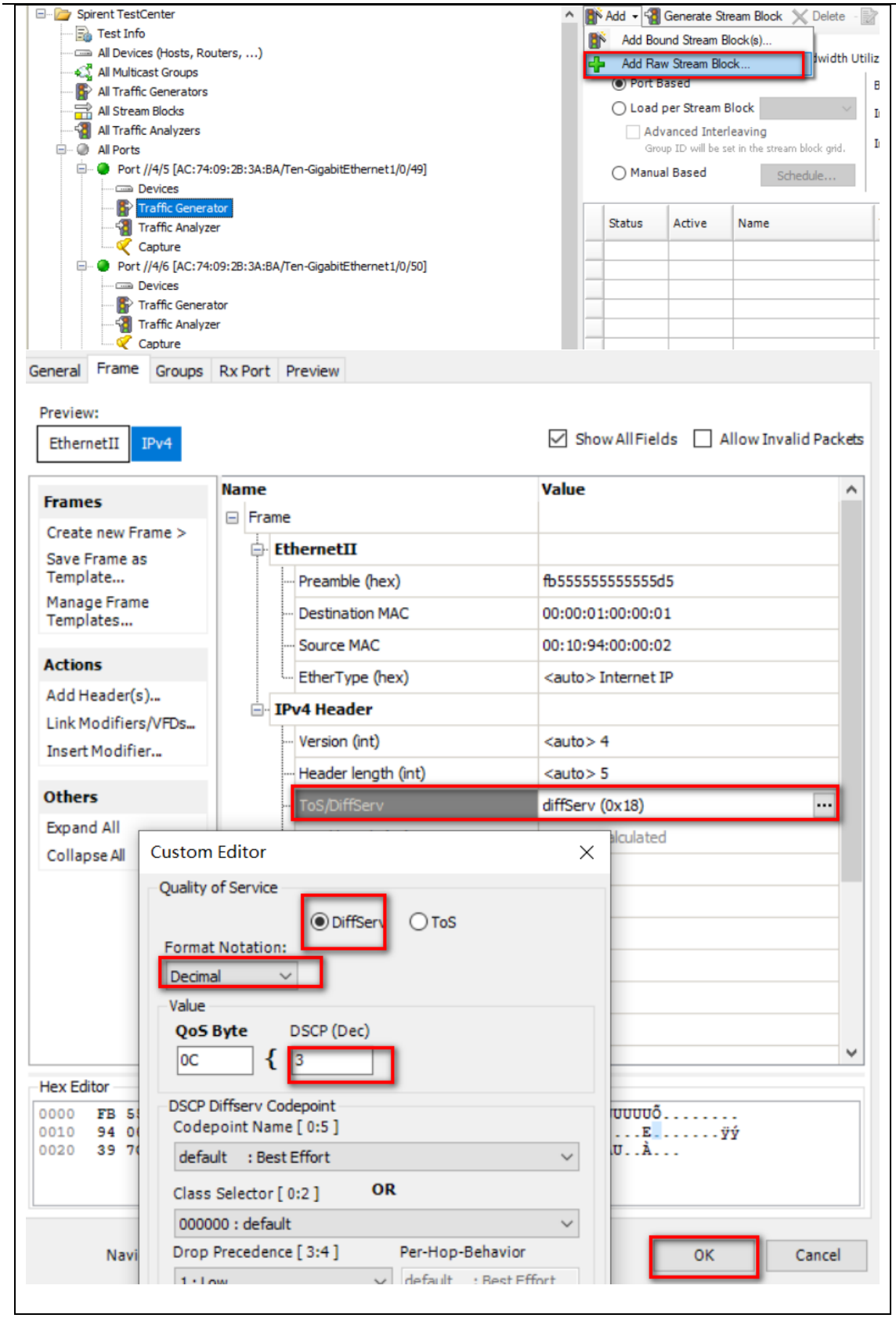


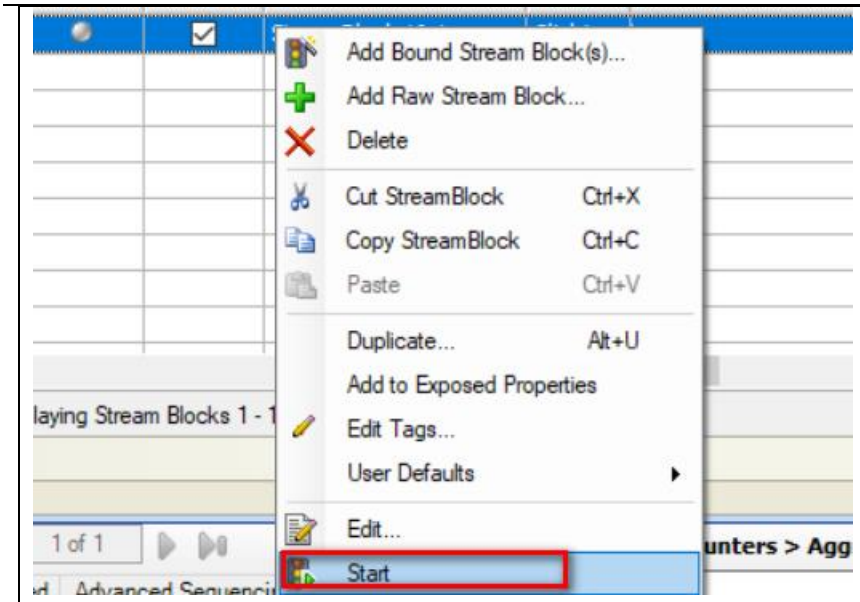


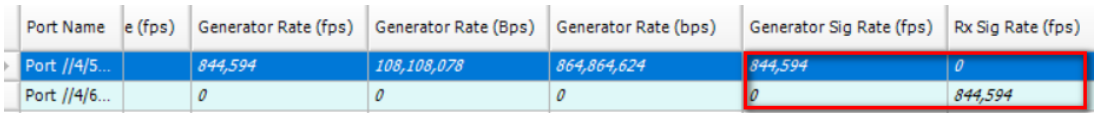
8. Clear the configuration and configure traffic classifier to match the traffic with DSCP 3, configure traffic behavior to remark it to 6, and configure the corresponding QoS policy.

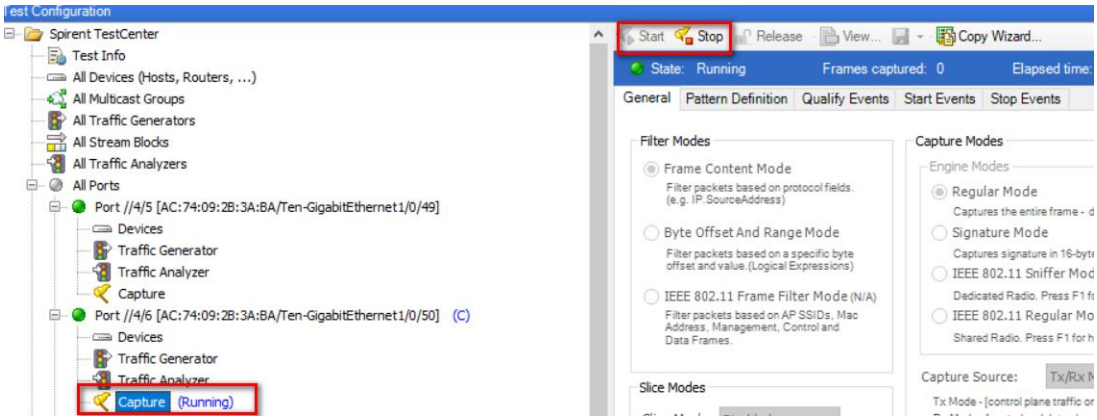
```
[DUT]acl advanced  3000
[DUT-acl-ipv4-adv-3000]display this
#
acl advanced 3000
 rule 0 permit ip dscp 3
#
return
[DUT-acl-ipv4-adv-3000]traffic classifier 3
[DUT-classifier-3]display this
#
traffic classifier 3 operator and
 if-match acl 3000
#
return
[DUT-classifier-3]traffic behavior 3
[DUT-behavior-3]display this
#
traffic behavior 3
 remark dscp 6
#
return
[DUT-behavior-3]qos policy 3
[DUT-qospolicy-3]display this
#
qos policy 3
 classifier 3 behavior 3
#
```

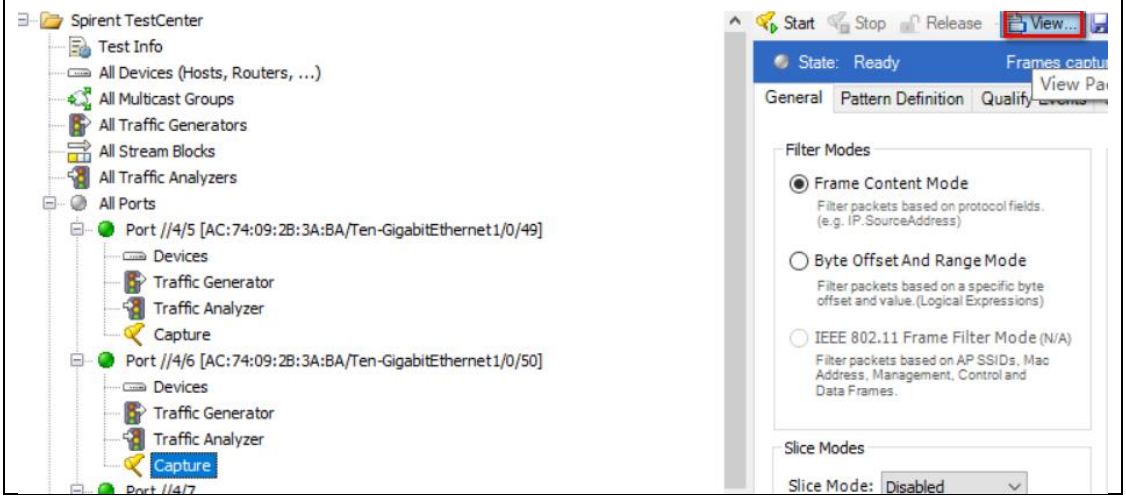
9. Send packets with DSCP 3. Result 3 is expected











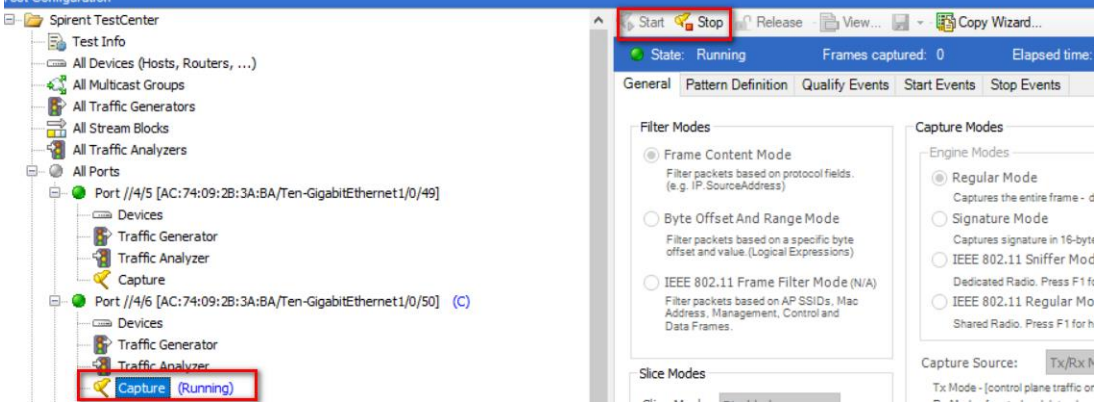
No.	Time	Source	Destination	Protocol	Length	Info
23176	0.027439	192.85.1.2	192.0.0.1	IPv4	128	Unknown (253)
23177	0.027440	192.85.1.2	192.0.0.1	IPv4	128	Unknown (253)
23178	0.027441	192.85.1.2	192.0.0.1	IPv4	128	Unknown (253)
23179	0.027443	192.85.1.2	192.0.0.1	IPv4	128	Unknown (253)
23180	0.027444	192.85.1.2	192.0.0.1	IPv4	128	Unknown (253)
23181	0.027445	192.85.1.2	192.0.0.1	IPv4	128	Unknown (253)
23182	0.027446	192.85.1.2	192.0.0.1	IPv4	128	Unknown (253)
23183	0.027447	192.85.1.2	192.0.0.1	IPv4	128	Unknown (253)
23184	0.027448	192.85.1.2	192.0.0.1	IPv4	128	Unknown (253)
23185	0.027450	192.85.1.2	192.0.0.1	IPv4	128	Unknown (253)
23186	0.027451	192.85.1.2	192.0.0.1	IPv4	128	Unknown (253)

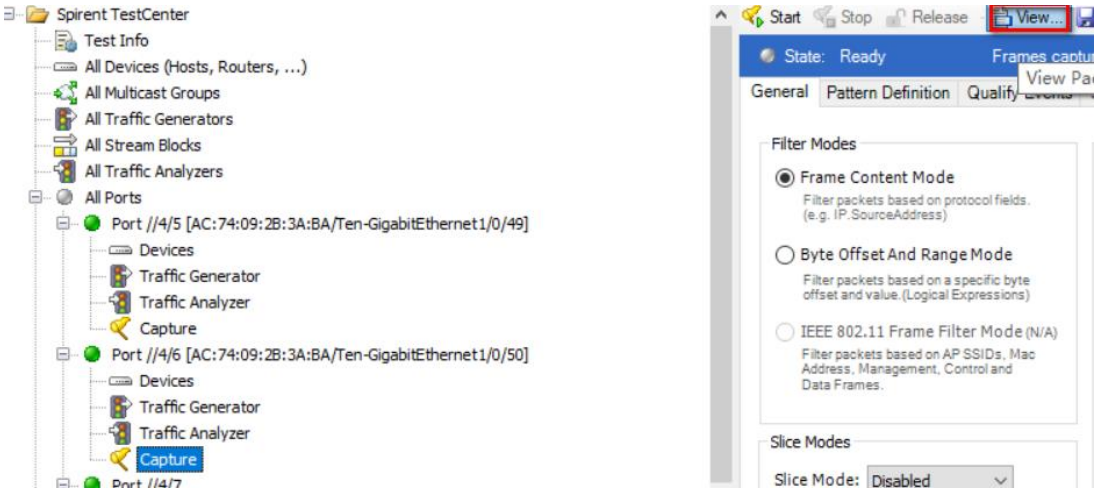
```
> Frame 1: 128 bytes on wire (1024 bits), 128 bytes captured (1024 bits) on interface \\.\pipe\view_capture_192-168-207-244_4_6_01222021_101526, id 0
> Ethernet II, Src: Performa_00:00:02 (00:10:94:00:00:02), Dst: Xerox_00:00:01 (00:00:01:00:00:01)
v Internet Protocol Version 4, Src: 192.85.1.2, Dst: 192.0.0.1
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  v Differentiated Services Field: 0x0c (DSCP: Unknown, ECN: Not-ECT)
      0000 11.. = Differentiated Services Codepoint: Unknown (3)
      .... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
```

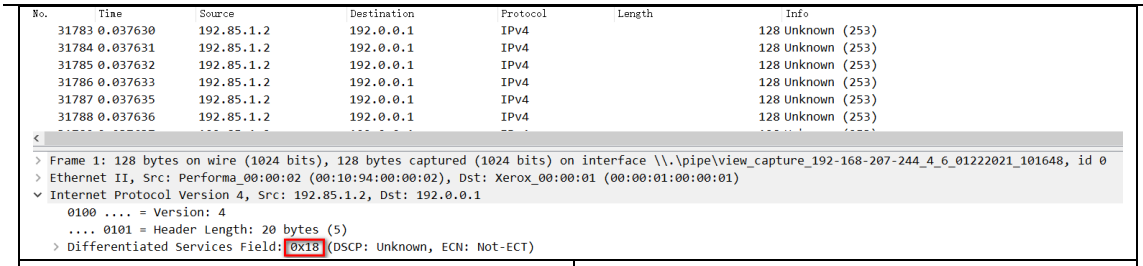
10. Apply QoS policy to Port 1. Result 4 is expected

```
[DUT-Ten-GigabitEthernet1/0/49]qos apply policy 3 inbound
```

Port Name	e (fps)	Generator Rate (fps)	Generator Rate (Bps)	Generator Rate (bps)	Generator Sig Rate (fps)	Rx Sig Rate (fps)
Port //4/5...		844,594	108,108,078	864,864,624	844,594	0
Port //4/6...		0	0	0	0	844,594







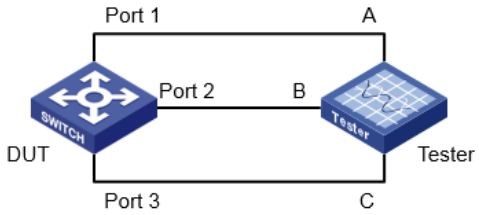
☐ Passed	☐ Failed

5.4 QoS

Test Item Name: QoS

Work Hour: 40 min

Test Topology:



Test Process:

1. Configure IPv4 ACLs, traffic classes, traffic behaviors, and QoS policies.
2. Send packets with source IPv4 addresses 10.10.10.20 and 10.10.10.21 to Port 1 of DUT 1 at a rate of 500 Mbps. Result 1 is expected.
3. Apply QoS policy p1 to Port 1. Result 2 is expected.
4. Send packets with source IPv4 address other than 10.10.10.20 and 10.10.10.21 to Port 1 of DUT 1. Result 3 is expected.
5. Configure IPv6 ACLs, traffic classes, traffic behaviors, and QoS policies.
6. Send packets with source IPv6 addresses 2001:1::1 and 2001:1::2 to Port 1 of DUT 1 at a rate of 500 Mbps. Result 4 is expected.
7. Apply QoS policy p1 to Port 1. Result 5 is expected.
8. Send packets with source IPv4 address other than 2001:1::1 and 2001:1::2 to Port 1 of DUT 1. Result 3 is expected.

Expect Results:

1. Port 2 receives all packets with source IPv4 addresses 10.10.10.20 and 10.10.10.21.
2. Port 2 receives packets with source IPv4 addresses 10.10.20 and 10.10.10.21 at a total rate of 3072 kbps.
3. Port 2 receives packets at wire speed.
4. Port 2 receives all packets with source IPv6 addresses 2001:1::1 and 2001:1::2.
5. Port 2 receives packets with source IPv6 addresses 2001:1::1 and 2001:1::2 at a total rate of 3072 kbps.

Actual Result：

1. Configure acl

#

acl advanced 3001

rule 0 permit ip source 10.10.10.20 0

#

acl advanced 3002

rule 0 permit ip source 10.10.10.21 0

#

2. Configure traffic classifier and traffic behavior

#

traffic classifier 1 operator and

if-match acl 3001

#

traffic classifier 2 operator and

if-match acl 3002

#

traffic behavior 1

car cir 1024 cbs 64000 ebs 0 green pass red discard yellow pass

#

traffic behavior 2

car cir 2048 cbs 128000 ebs 0 green pass red discard yellow pass

#

3. Configure QOS policy to bound them

#

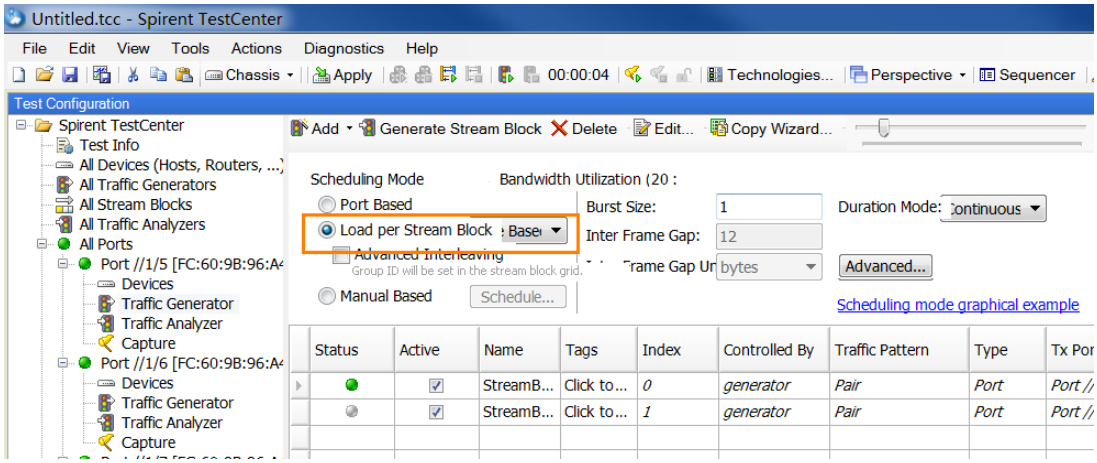
qos policy 1

classifier 1 behavior 1

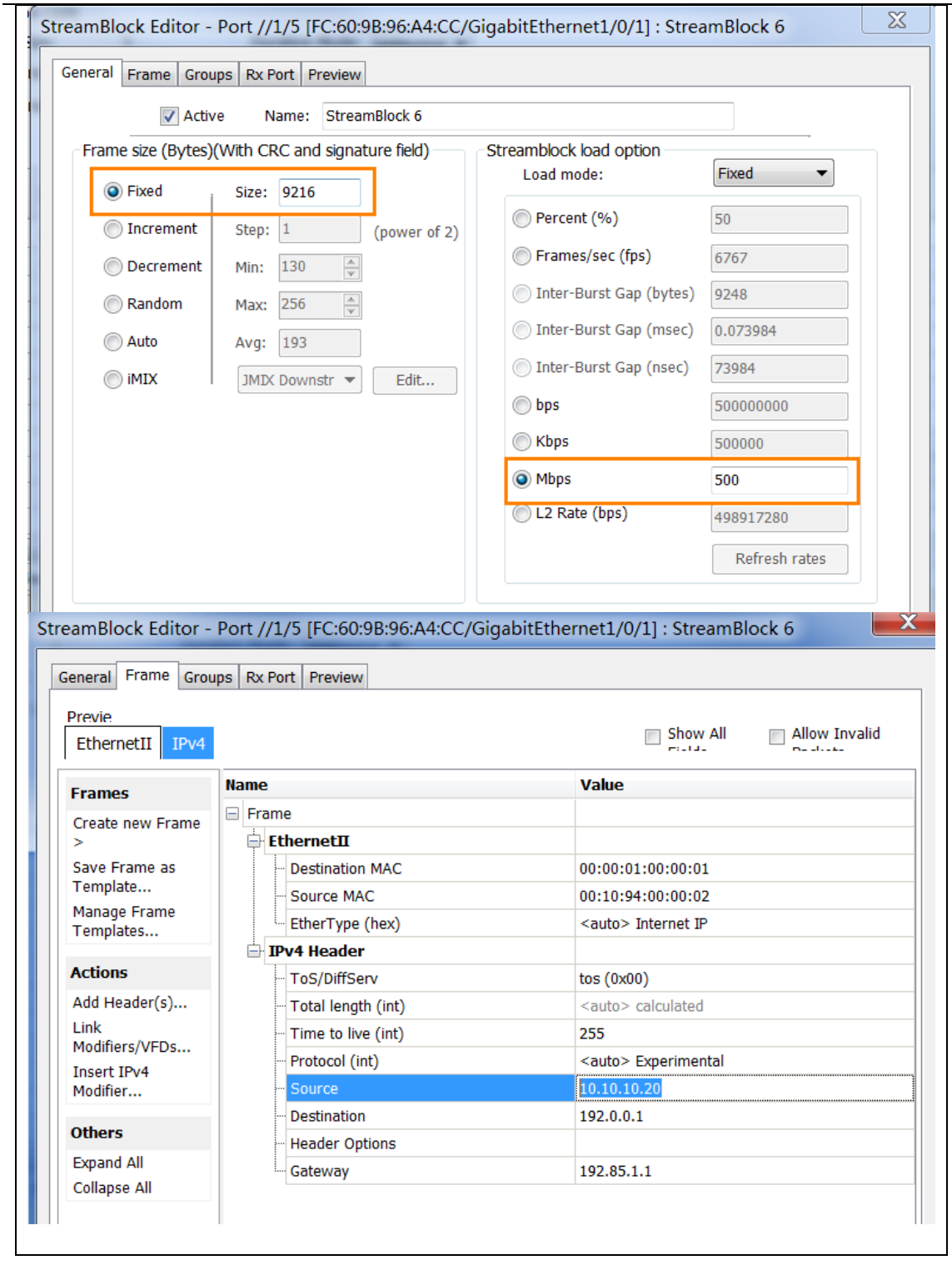
classifier 2 behavior 2

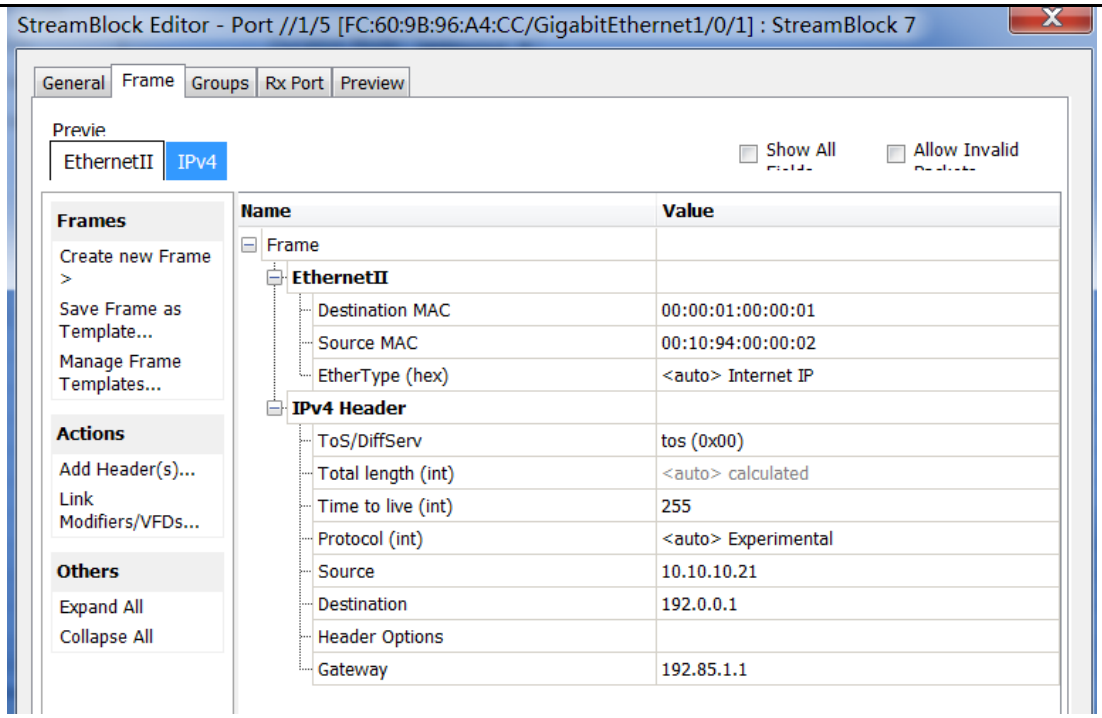
#

4. Change the scheduling mode to **load per stream block**

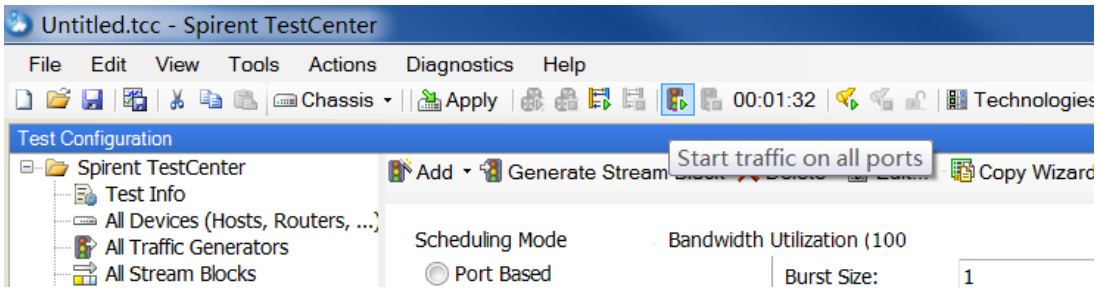


5. Create traffic with source IP 10.10.10.20 and 10.10.10.21

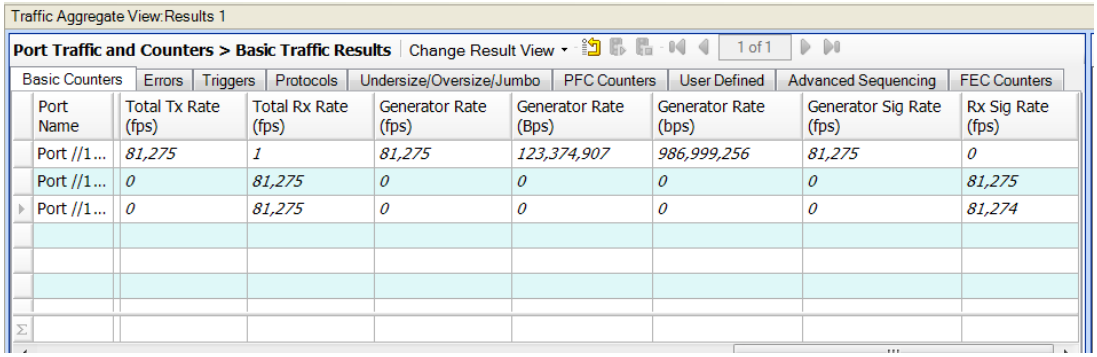




6. Start the traffic



7. All the traffic is received on Port B



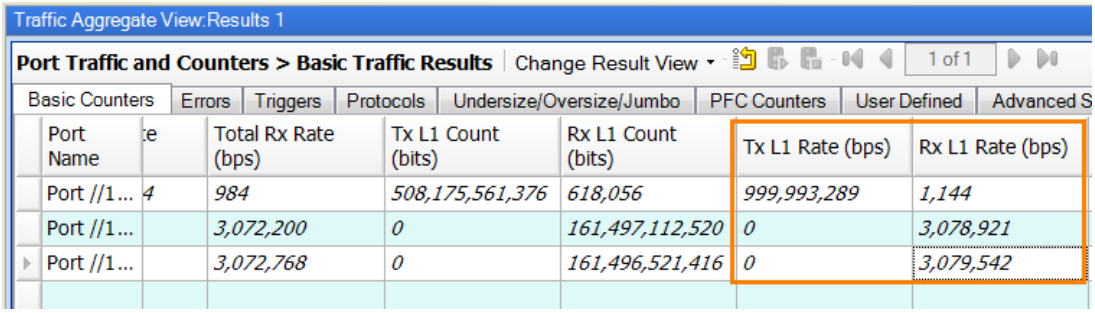
8. Apply the qos policy on Port 1

#

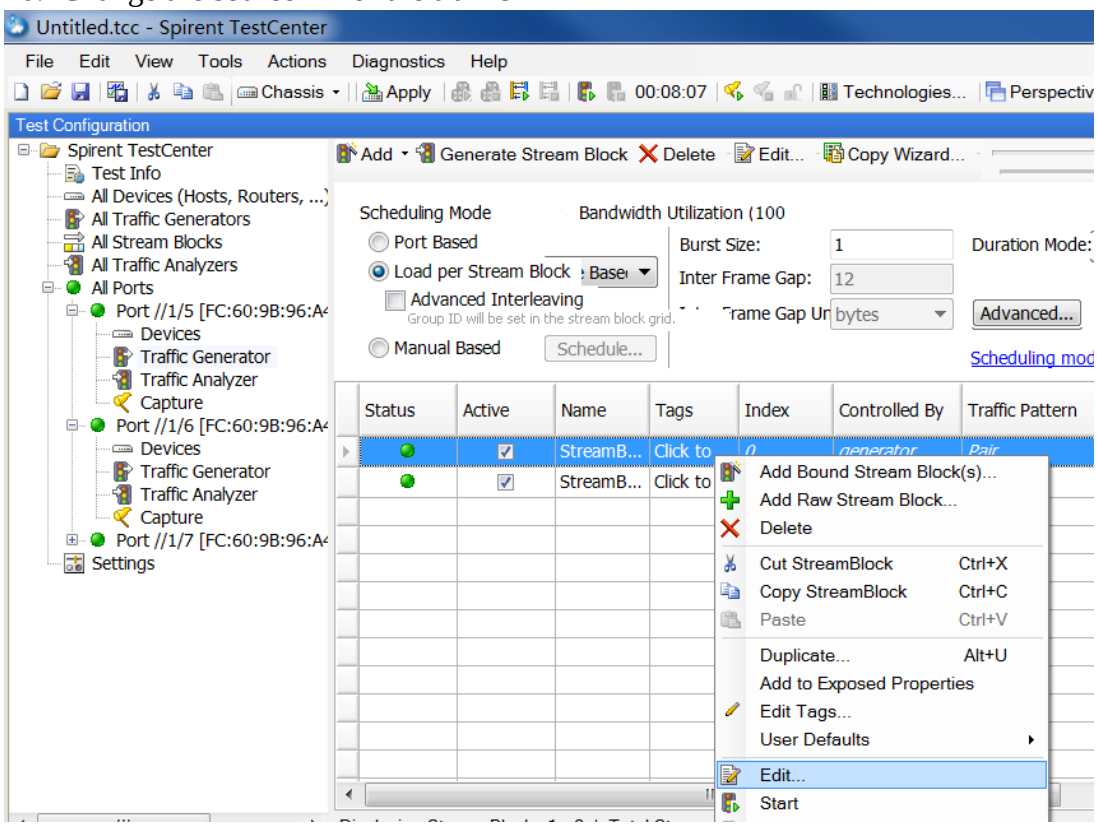
interface GigabitEthernet1/0/1

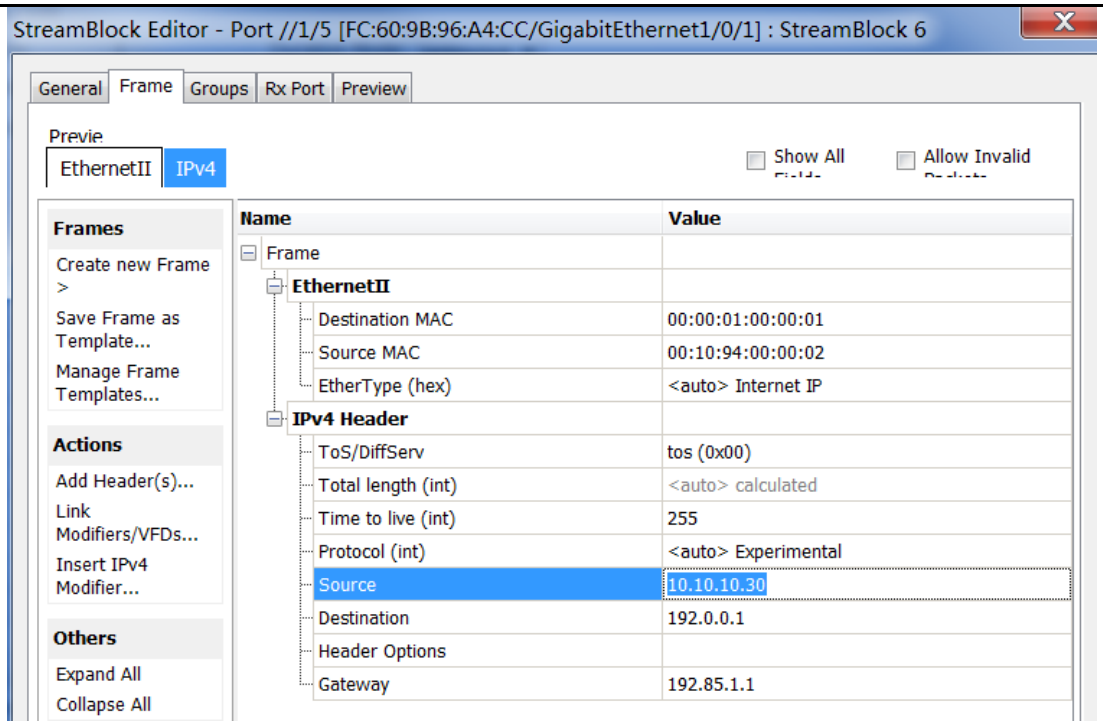
port link-mode bridge
qos apply policy 1 inbound
#

9. The traffic speed is limited to around 3072kbps

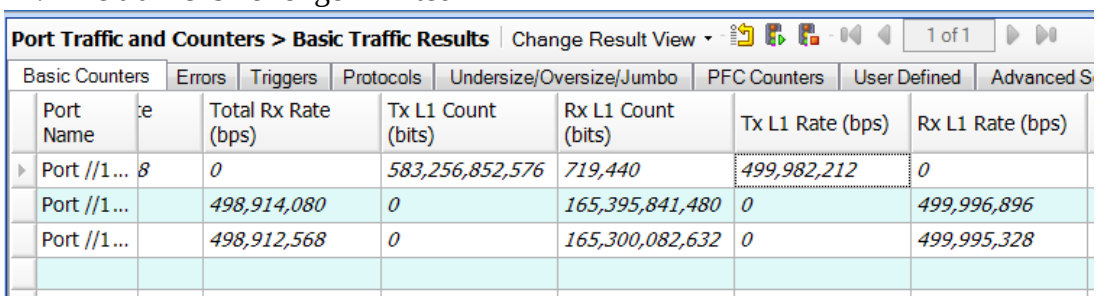


10. Change the source IP for the traffic





11. The traffic is no longer limited



12. Then check IPv6 qos function

Configuration for IPv6：

#

acl ipv6 advanced 3003

rule 0 permit ipv6 source 2001:1::1/128

#

acl ipv6 advanced 3004

rule 0 permit ipv6 source 2001:1::2/128

#

traffic classifier 3 operator and

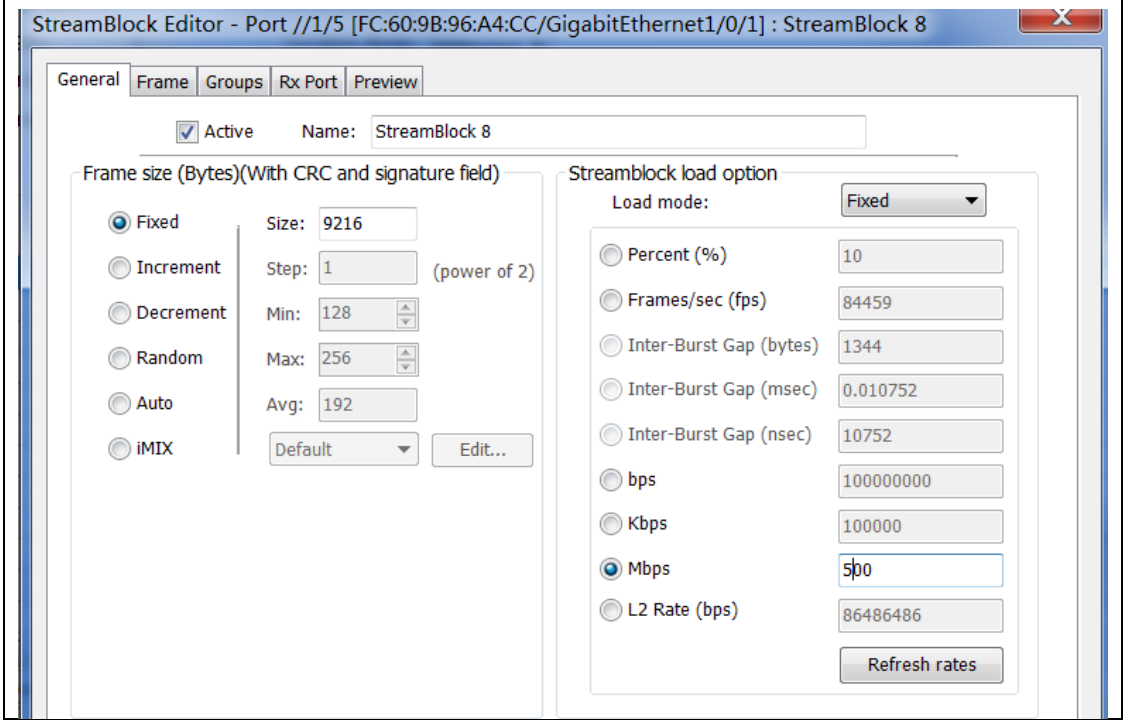
if-match acl ipv6 3003

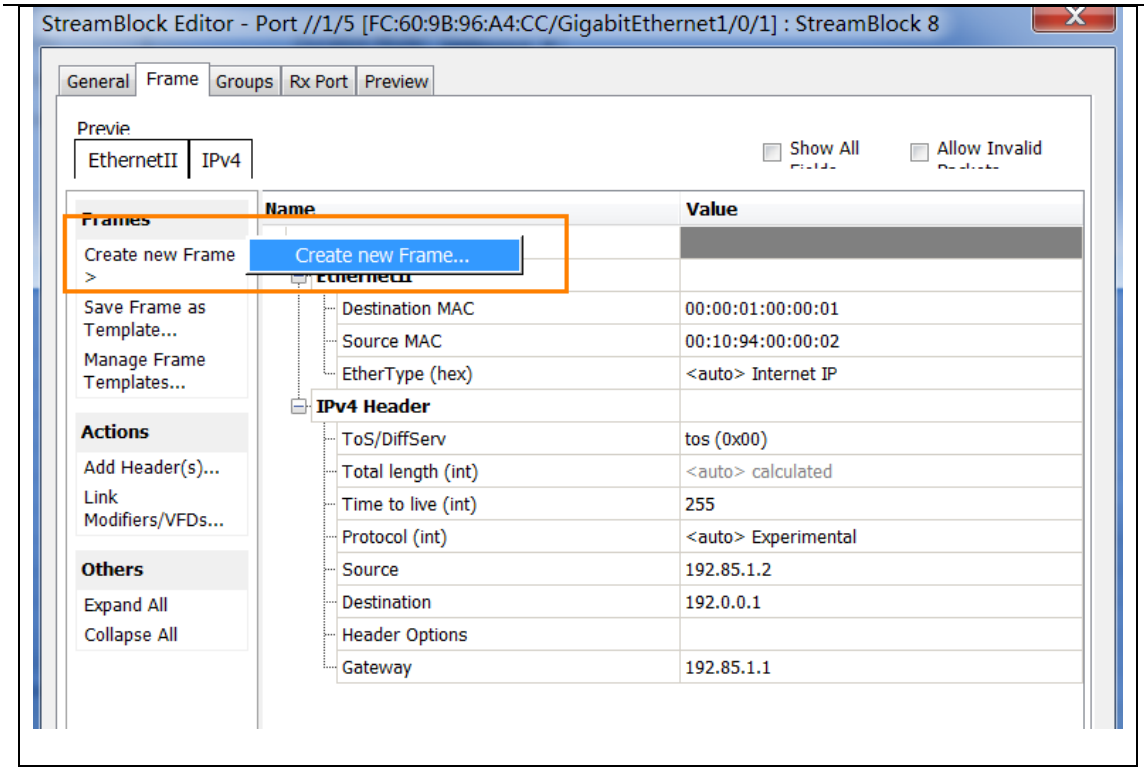
#

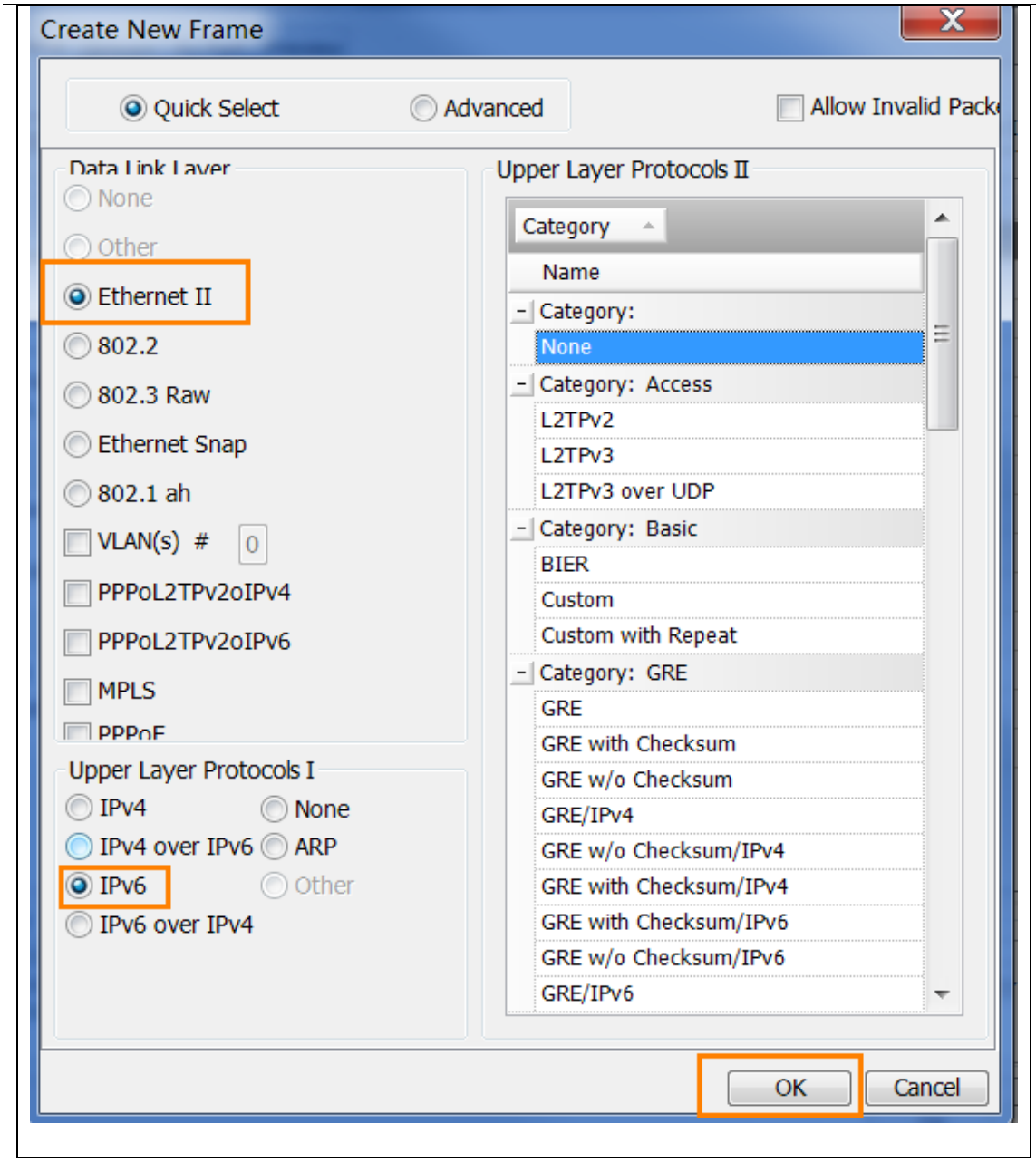
traffic classifier 4 operator and

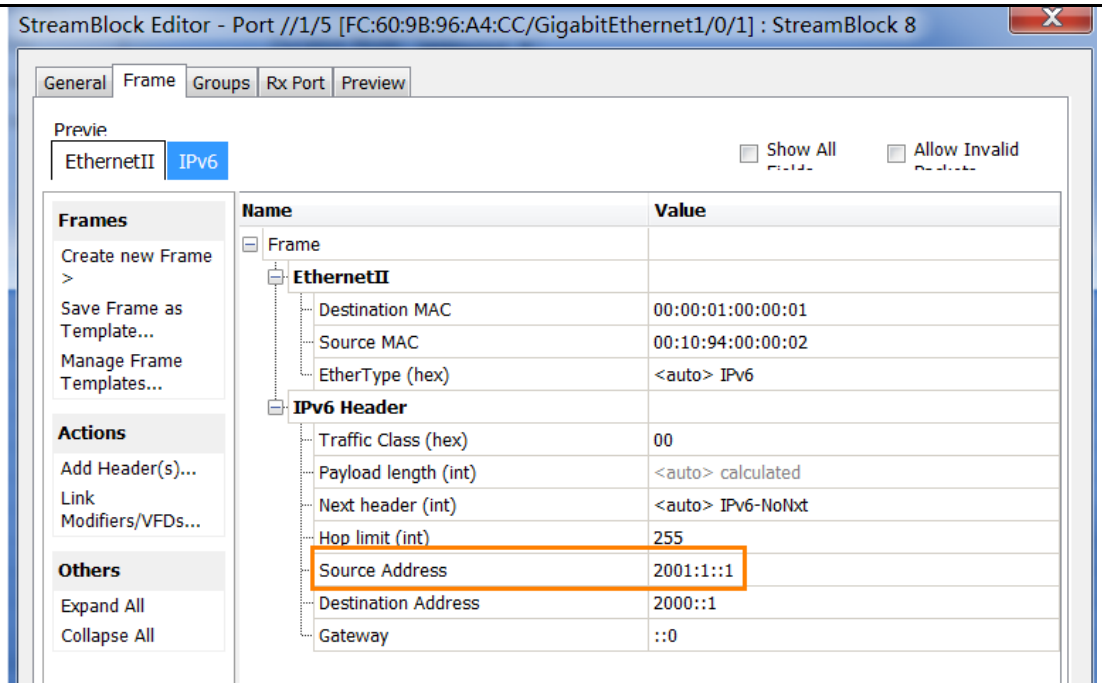
```
 if-match acl ipv6 3004
#
traffic behavior 3
 car cir 2048 cbs 128000 ebs 0 green pass red discard yellow pass
#
traffic behavior 4
 car cir 1024 cbs 64000 ebs 0 green pass red discard yellow pass
#
qos policy 2
 classifier 3 behavior 3
 classifier 4 behavior 4
#
```

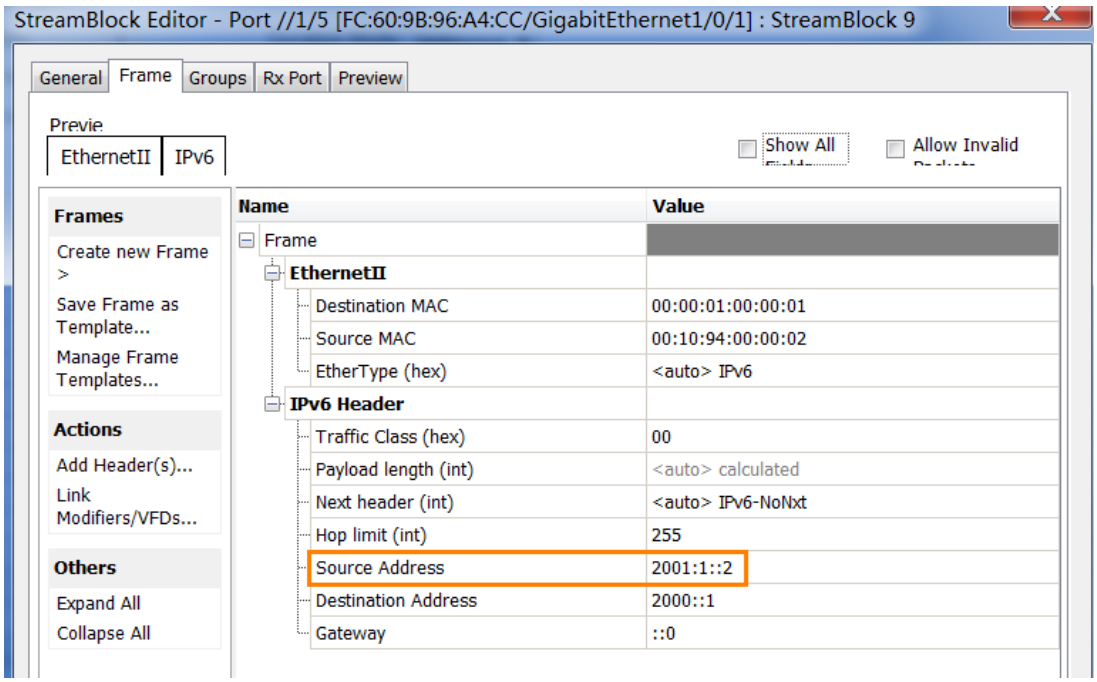
13. Create traffic with IPv6 source 2001:1::1 and 2001:1::2



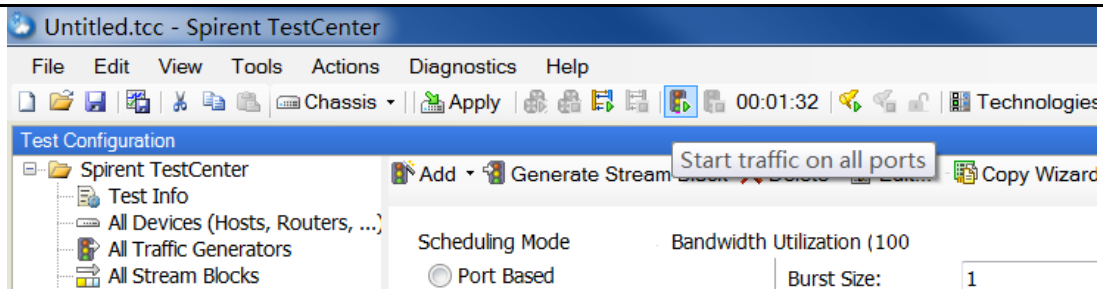




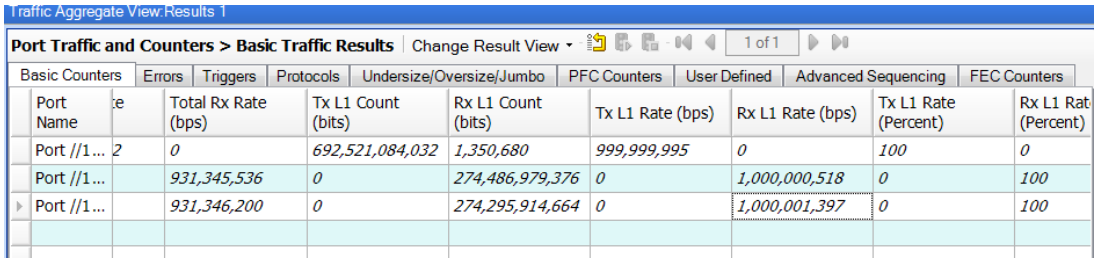




14. Start all the traffic



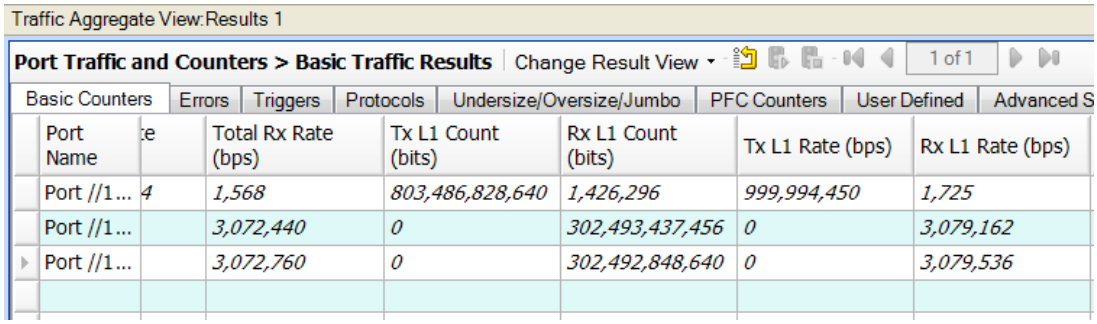
15. All the traffic is received



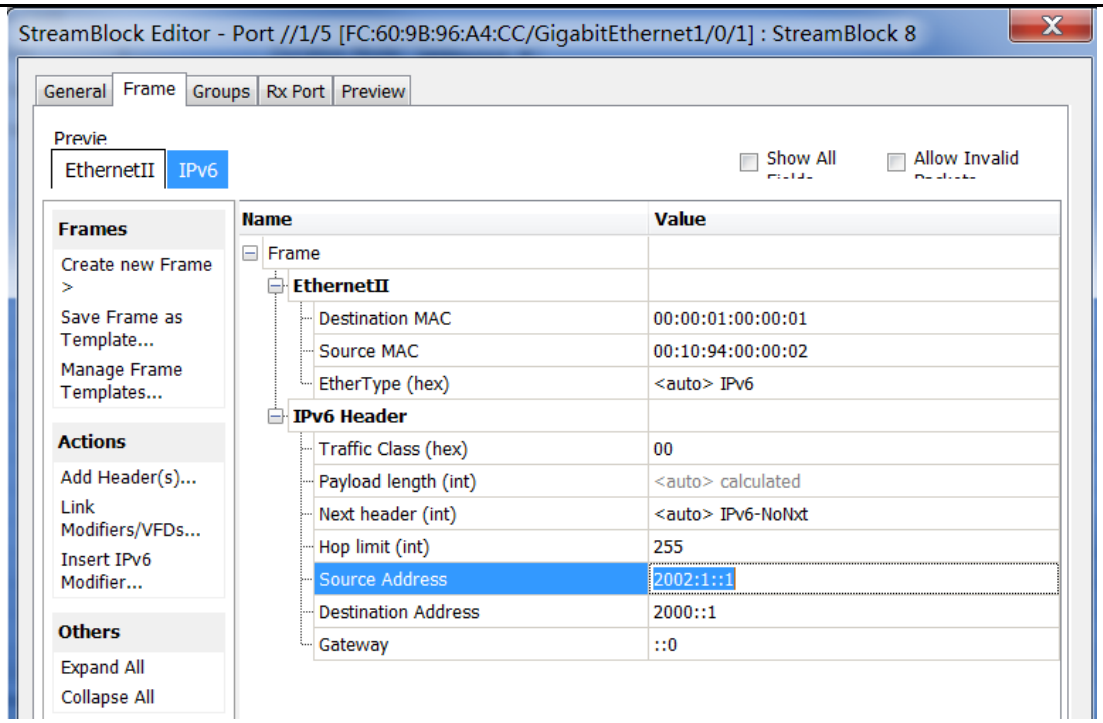
16. Apply the qos policy on Port 1

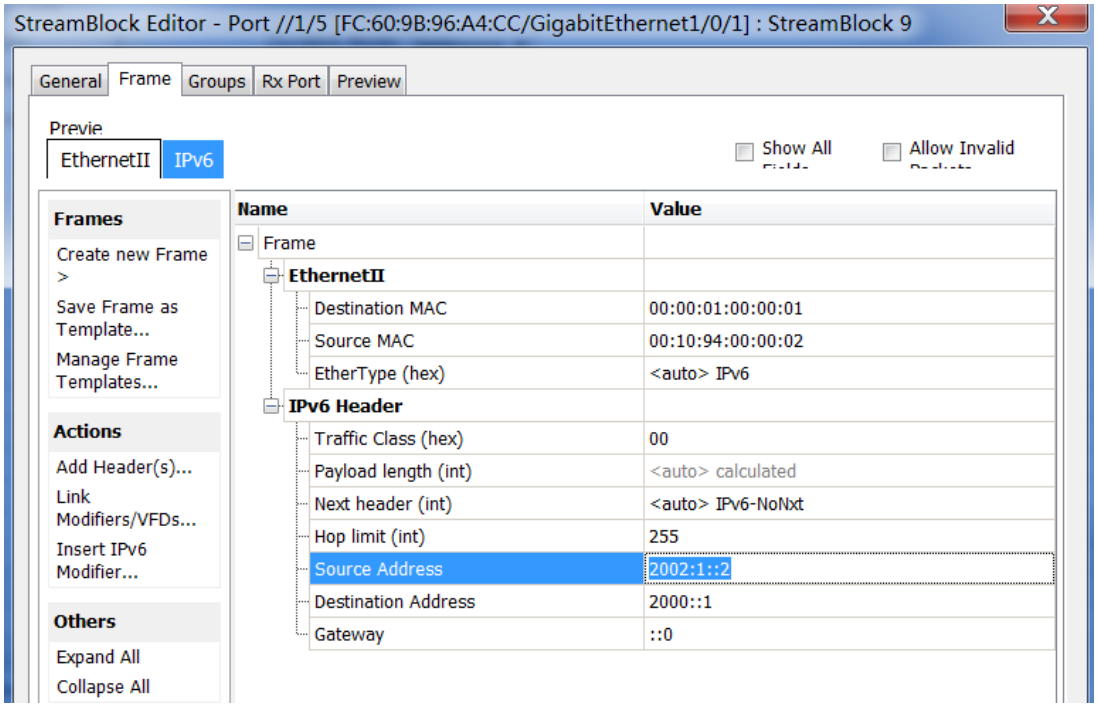
#
interface GigabitEthernet1/0/1
port link-mode bridge
qos apply policy 2 inbound
#

17. Traffic is limited



18. Change the source IP





19. Traffic is no more limited

Port Traffic and Counters > Basic Traffic Results | Change Result View | 1 of 1

Basic Counters | Errors | Triggers | Protocols | Undersize/Oversize/Jumbo | PFC Counters | User Defined | Advanced Sequencing | FEC Counters

Port Name	te	Total Rx Rate (bps)	Tx L1 Count (bits)	Rx L1 Count (bits)	Tx L1 Rate (bps)	Rx L1 Rate (bps)	Tx L1 Rate (Percent)	Rx L1 Rat (Percent)
Port //1...	8	0	863,016,986,368	1,496,736	1,000,005,897	0	100.001	0
Port //1...		997,844,192	0	326,714,588,288	0	1,000,009,762	0	100.001
Port //1...		997,840,720	0	326,532,820,920	0	1,000,006,228	0	100.001

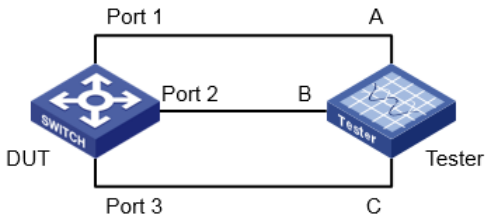
☐ Passed	☐ Failed

5.5 SP+WRR queuing

Test Item Name: SP+WRR queuing

Work Hour：45 min

Test Topology:

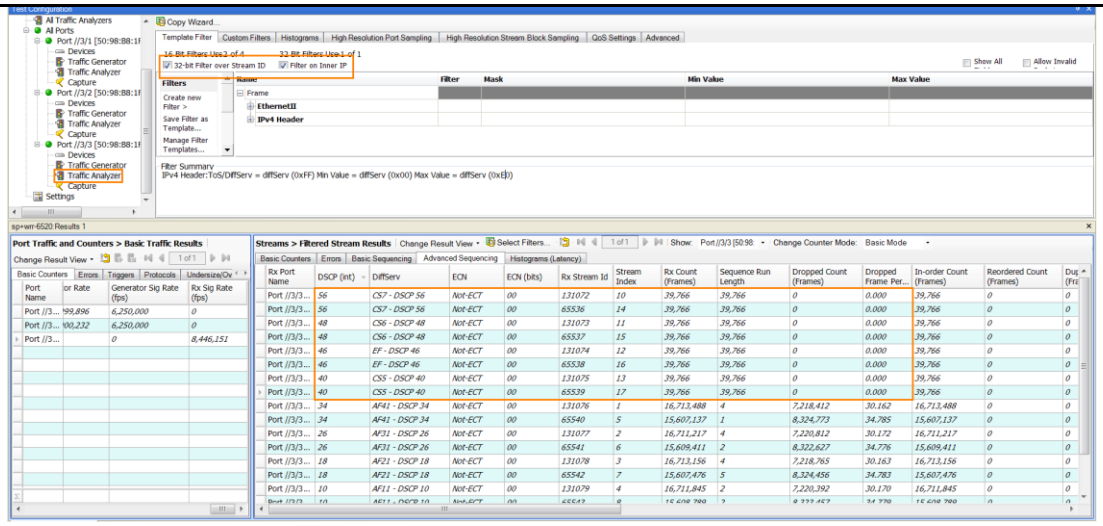


Test Process:

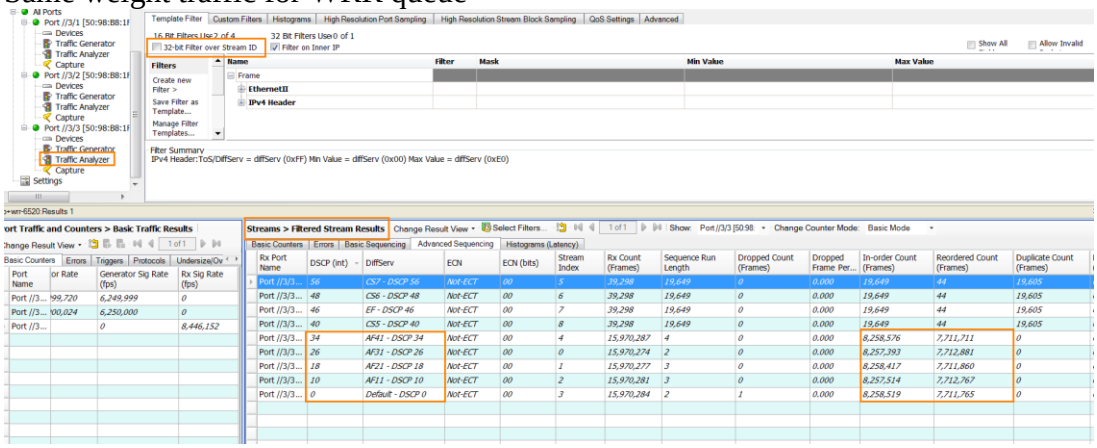
1. Configure Port 1, Port 2, and Port 3 as trunk ports, and assign them to vlan 3
2. Configure the priority trust mode as dot1p on Port 1 and Port 2, and configure SP+WRR on Port 3. Queue 6 and queue 7 are SP queues. Queues 0 to 5 are WRR queues, with scheduling weights as 1, 2, 3, 4, 5, and 9, respectively.
3. Make Port 3 learn the MAC address 1-1-1.
4. Send traffic from Port A and Port B, with dot1p increasing from 0 to 7, with expected result 1.

Expect Results:

1. Port 3 receives all packets of queue 6 and queue 7. Other packets share the remaining 40% of bandwidth according to their scheduling weights. No traffic loss on SP queue



Same weight traffic for WRR queue



Actual Result:

1. Configuration on DUT

```
#
vlan 3
#
qos map-table dot1p-lp
 import 0 export 0
 import 1 export 1
 import 2 export 2
#
interface Ten-GigabitEthernet1/0/25------port 1
 port link-type trunk
 port trunk permit vlan 1 3
 qos trust dscp
#
interface Ten-GigabitEthernet1/0/26-----port 2
 port link-type trunk
```

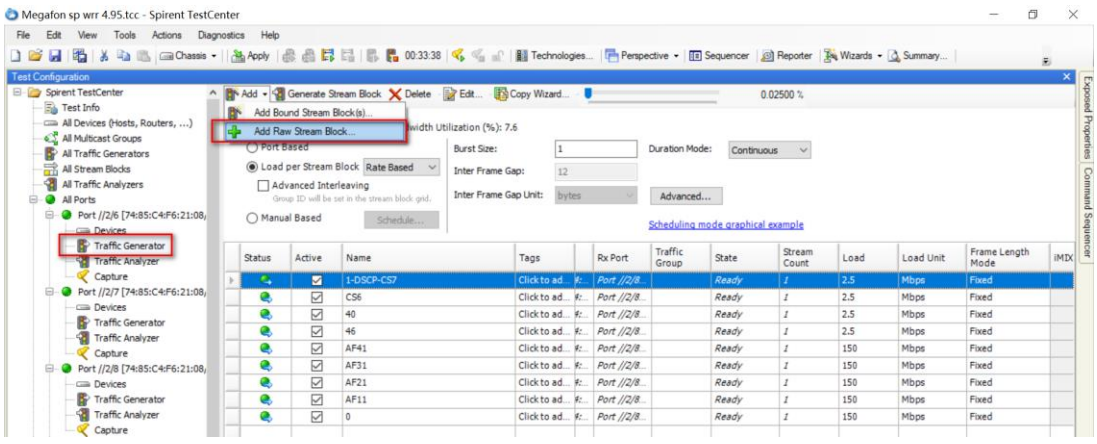
```
 port trunk permit vlan 1 3
 qos trust dscp
#
interface Ten-GigabitEthernet1/0/27-----port 3
 port link-type trunk
 port trunk permit vlan 1 3
 qos trust dscp
 qos wrr af1 group 1 weight 1
 qos wrr af2 group 1 weight 1
 qos wrr af3 group 1 weight 1
 qos wrr af4 group 1 weight 1
 qos wrr ef group sp
 qos wrr cs6 group sp
 qos wrr cs7 group sp
#
```

2. Make Port 3 learn the MAC address 1-1-1.

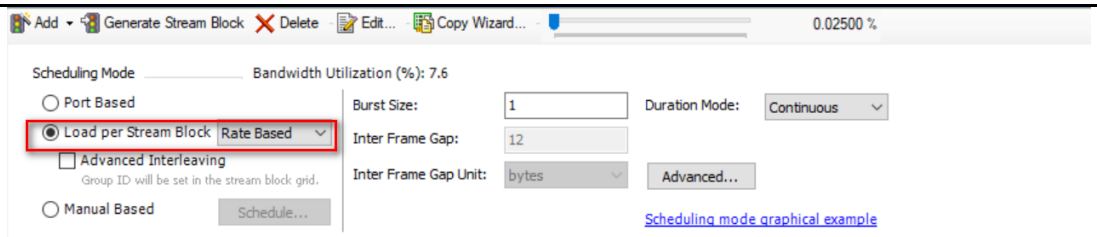
3. Send traffic from Port A and Port B, with dot1p increasing from 0 to 7, with expected result 1

```
interface Ten-GigabitEthernet1/0/27
 port link-mode bridge
 port link-type trunk
 port trunk permit vlan 1 3
 mac-address static 0001-0001-0001 vlan 3
 qos trust dscp
 qos wrr af1 group 1 weight 1
 qos wrr af2 group 1 weight 1
 qos wrr af3 group 1 weight 1
 qos wrr af4 group 1 weight 1
 qos wrr ef group sp
 qos wrr cs6 group sp
 qos wrr cs7 group sp
#
```

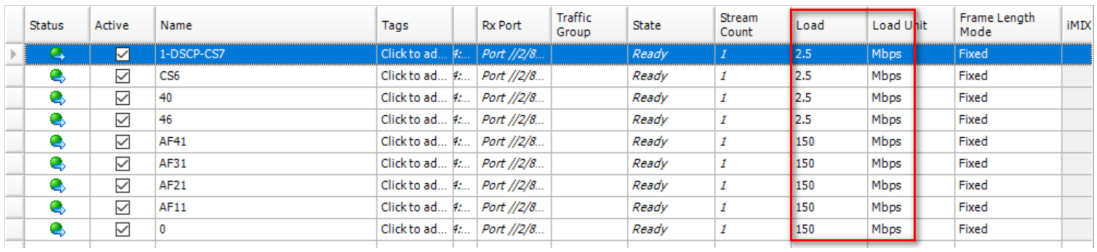
Add 9 streams and edit



before configuring streams, choose Load per Stream Block

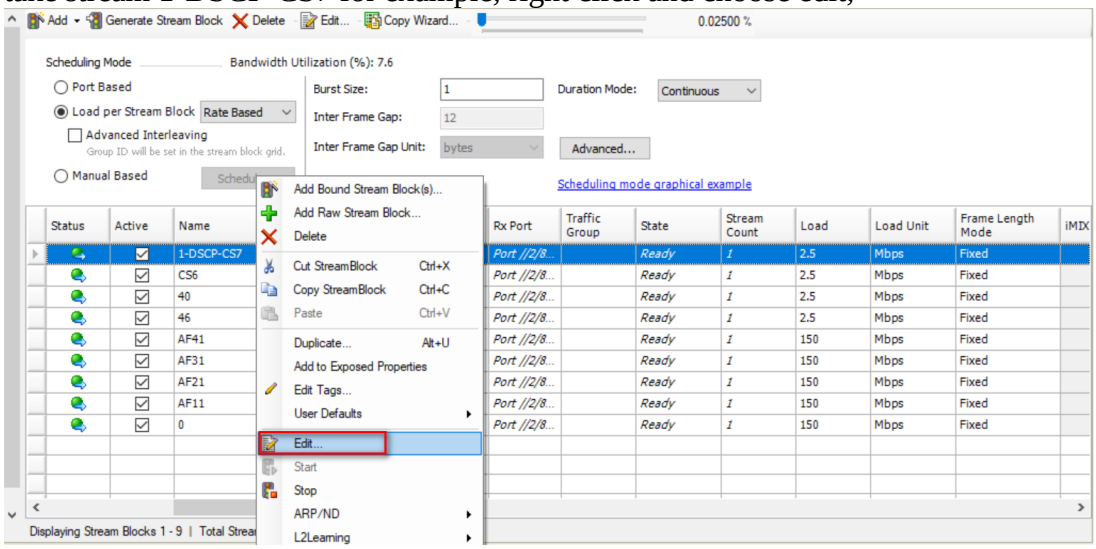


edit 9 streams

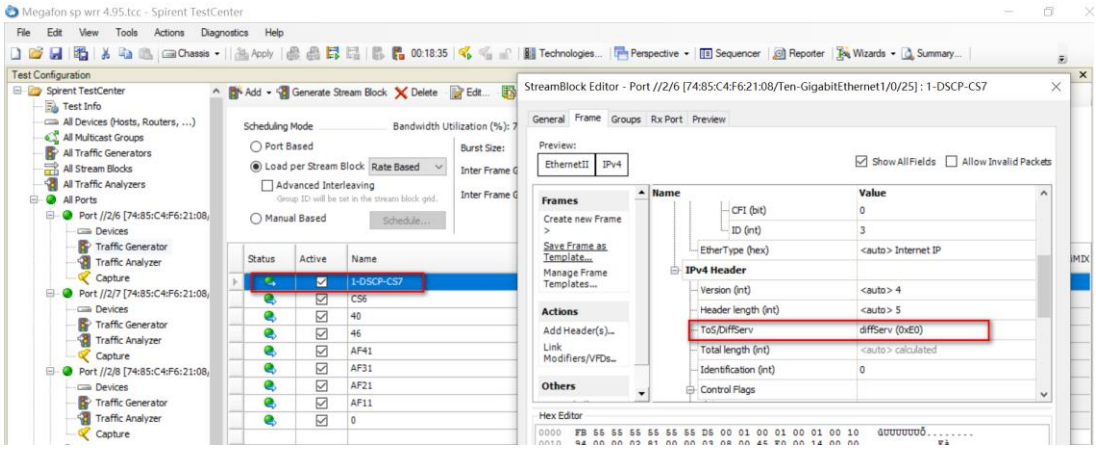


Status	Active	Name	Tags	Rx Port	Traffic Group	State	Stream Count	Load	Load Unit	Frame Length Mode	iMIX
	☑	1-DSCP-CS7	Click to ad...	Port //2/8...		Ready	1	2.5	Mbps	Fixed	
	☑	CS6	Click to ad...	Port //2/8...		Ready	1	2.5	Mbps	Fixed	
	☑	40	Click to ad...	Port //2/8...		Ready	1	2.5	Mbps	Fixed	
	☑	46	Click to ad...	Port //2/8...		Ready	1	2.5	Mbps	Fixed	
	☑	AF41	Click to ad...	Port //2/8...		Ready	1	150	Mbps	Fixed	
	☑	AF31	Click to ad...	Port //2/8...		Ready	1	150	Mbps	Fixed	
	☑	AF21	Click to ad...	Port //2/8...		Ready	1	150	Mbps	Fixed	
	☑	AF11	Click to ad...	Port //2/8...		Ready	1	150	Mbps	Fixed	
	☑	0	Click to ad...	Port //2/8...		Ready	1	150	Mbps	Fixed	

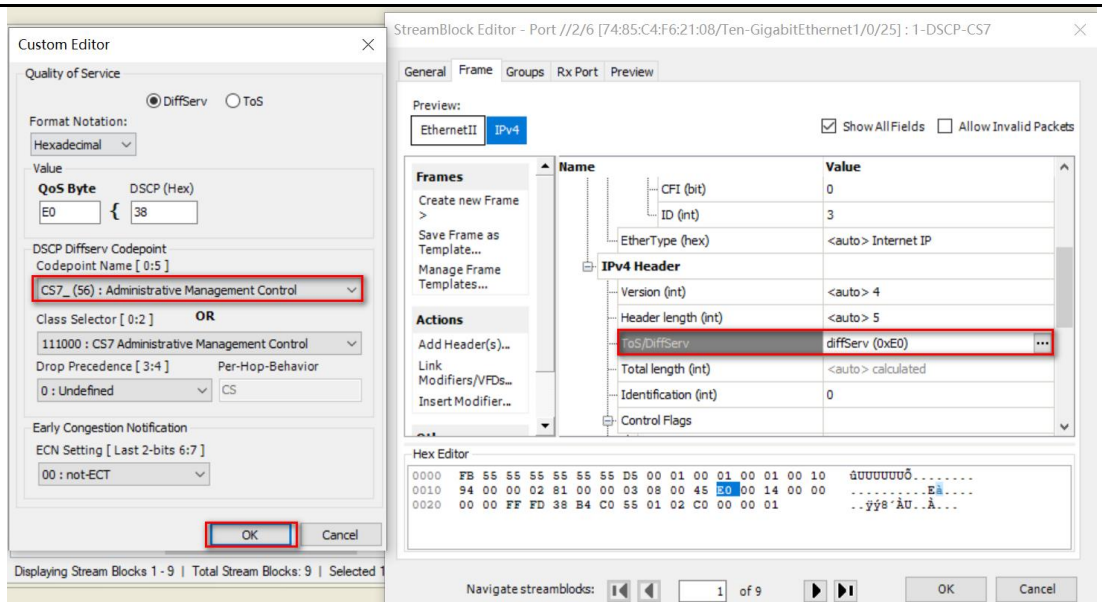
take stream 1-DSCP-CS7 for example, right click and choose edit,



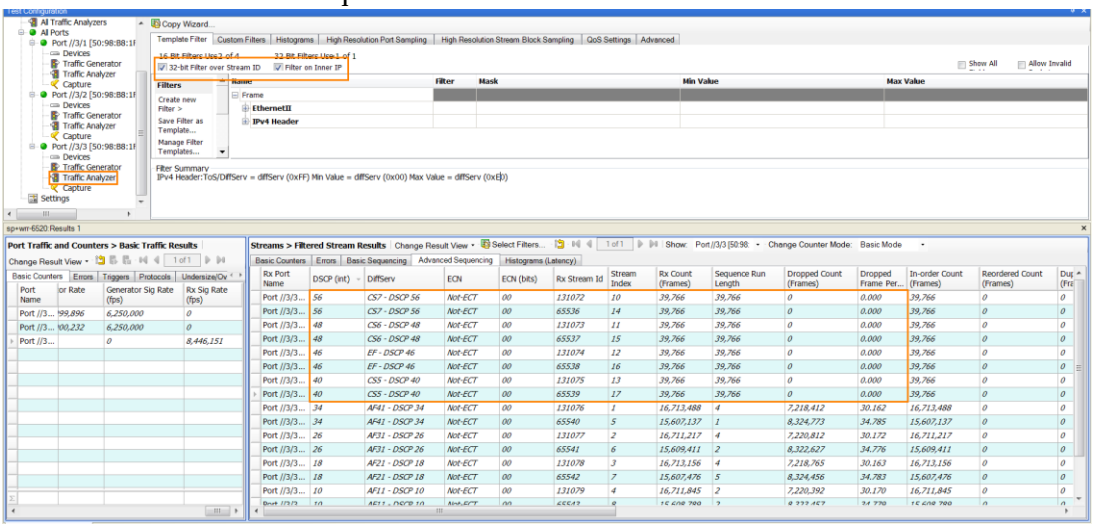
choose Frame and choose ToS/Differv



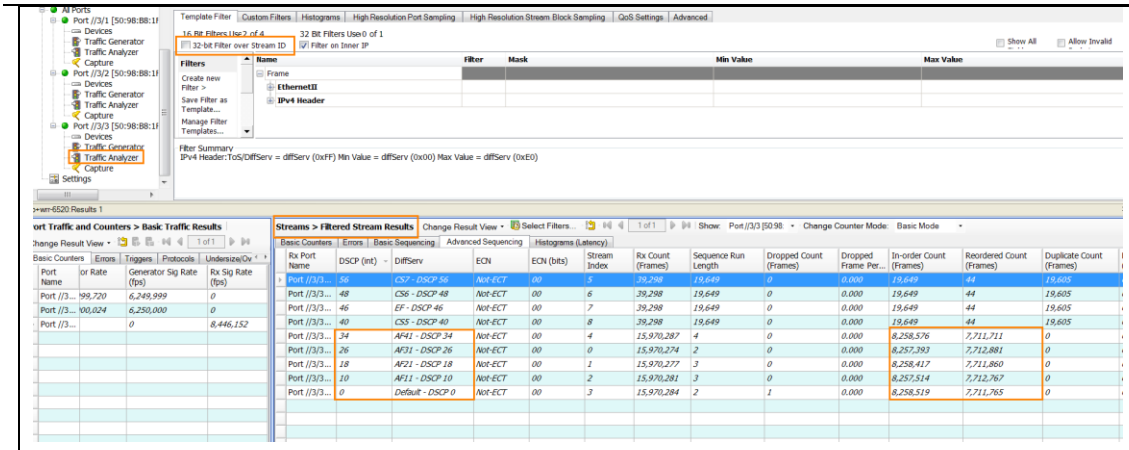
choose CS7 like the following picture,



No traffic loss on SP queue



Same weight traffic for WRR queue



☐ Passed	☐ Failed