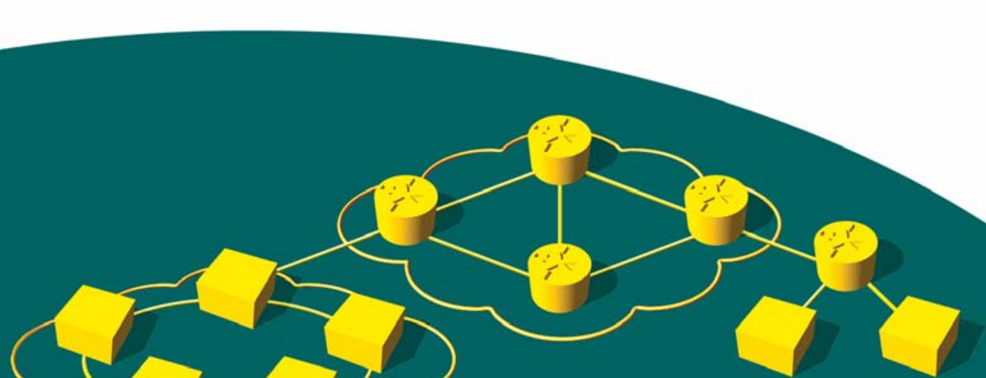
Spirent Communications
Step-By-Step Test Methodologies

TRT Edition: Protocol Independent Multicast (PIM)

December 2004



P/N 340-5120-001 REV A

Spirent Communications, Inc.

26750 Agoura Road
Calabasas, CA
91302 USA

Support Contacts

U.S.
E-mail: support@spirentcom.com
Web: http://support.spirentcom.com
Toll Free: 1-800-SPIRENT (1-800-774-7368)
Phone: + 1 818-676-2616
Fax: +1 818-880-9154

Europe
E-mail: support.europe@spirentcom.com
Web: http://support.spirentcom.com
Phone: +33 (0) 1 61 37 22 70
Fax: +33 (0) 1 61 37 22 51

Limited Warranty

Spirent Communications, Inc. (“Spirent”) warrants that its Products will conform to the description on the face of order, that it will convey good title thereto, and that the Product will be delivered free from any lawful security interest or other lien or encumbrance.

Spirent further warrants to Customer that hardware which it supplies and the tangible media on which it supplies software will be free from significant defects in materials and workmanship for a period of twelve (12) months, except as otherwise noted, from the date of delivery (the “Warranty Period”), under normal use and conditions.

To the extent the Product is or contains software (“Software”), Spirent also warrants that the Software, if properly used by Licensee in accordance with the Software License Agreement, shall operate in material conformity with the specification for such Software for a period of ninety (90) days from the date of delivery (the “Warranty Period”). Spirent does not warrant that the functions contained in the Software will meet a specific requirement or that the operation will be uninterrupted or error free. Spirent shall have no warranty obligations whatsoever with respect to any Software which has been modified in any manner by Customer or any third party.

Defective Products and Software under warranty shall be, at Spirent's discretion, repaired or replaced or a credit issued to Customer's account for an amount equal to the price paid for such Product provided that: (a) such Product is returned to Spirent after first obtaining a return authorization number and shipping instructions, freight prepaid, to Spirent's location in the United States; (b) Customer provides a written explanation of the defect or Software failure claimed by Customer; and (c) the claimed defect actually exists and was not caused by neglect, accident, misuse, improper installation, improper repair, fire, flood, lightning, power surges, earthquake, or alteration. Spirent will ship repaired Products to Customer, freight prepaid. Except as otherwise stated, any claim on account of defective materials or for any other cause whatsoever will conclusively be deemed waived by Customer unless written notice thereof is given to Spirent within the Warranty Period. Spirent reserves the right to change the warranty and service policy set forth above at any time, after reasonable notice and without liability to Customer.

TO THE EXTENT PERMITTED BY APPLICABLE LAW, ALL IMPLIED WARRANTIES, INCLUDING BUT NOT LIMITED TO IMPLIED WARRANTIES OF MERCHANTABILITY, NONINFRINGEMENT AND FITNESS FOR A PARTICULAR PURPOSE, ARE HEREBY EXCLUDED, AND THE LIABILITY OF SPIRENT, IF ANY, FOR DAMAGE RELATING TO ANY ALLEGEDLY DEFECTIVE PRODUCT SHALL BE LIMITED TO THE ACTUAL PRICE PAID BY THE CUSTOMER FOR SUCH PRODUCT. THE PROVISIONS SET FORTH ABOVE STATE SPIRENT'S ENTIRE RESPONSIBILITY AND CUSTOMER'S SOLE AND EXCLUSIVE REMEDY WITH RESPECT TO ANY BREACH OF ANY WARRANTY.

Table of Contents

Introduction: PIM and PIM-SM

Creating Successful Multicast Streams

There are two fundamental components to creating successful multicast communications streams. The first component is the registration process that allows end-users to select and join multicast groups. The Internet Group Management Protocol (IGMP) typically facilitates this process. The second component is the routing process.

After the receivers join their respective groups, the network must deliver the multicast traffic to the correct end stations. In the Internet, a routing protocol must be used to dynamically calculate the appropriate forwarding paths to all registered receivers.

In addition, transmissions from the data source must be replicated at some point for the information to be received in multiple locations simultaneously. This delivery process is facilitated by a multicast routing protocol. The user can select from several multicast routing protocols, each with strengths and weaknesses.

The New Breed of Protocol

New multicast routing protocols developed in the late 1990s are collectively known as Protocol Independent Multicast (PIM). PIM comprises multicast forwarding protocols that are not dependent upon a specific unicast routing protocol (Multicast Open Shortest Path First, MOSPF, is a contradictory example and requires OSPF as the underlying unicast routing protocol).

In contrast to MOSPF, however, PIM takes advantage of existing routing and forwarding tables regardless of how they were constructed to forward multicast data.

PIM-SM for the Internet

PIM has several versions. The most common is PIM Sparse Mode (PIM-SM). PIM-SM is well suited for the Internet since it is designed to minimize the overhead and bandwidth requirements for multicast data streams.

PIM-SM exists exclusively between routers. Host computers (sources or receivers) do not participate in this protocol. PIM-SM shares common characteristics of other routing protocols such as discovery messages, topology information, and error detection and notification. PIM-SM also differs from traditional protocols since it does not facilitate exchanges of routing databases.

PIM-SM routers periodically generate “Hello” messages to discover and maintain stateful sessions with their neighbors. These multicast messages use the dedicated address of 224.0.0.13. After neighbors are discovered, PIM-SM routers signal their intentions to join specific multicast groups. This is accomplished by having a downstream router send an explicit PIM-SM “join” message (not to be confused with IGMP or MLD “join” messages) to an upstream router. The PIM-SM “join” message will specify the group and the source (if applicable) that the router wants to join, represented with a $(*,G_1)$ or (S_1,G_1) notation. Upstream routers can then forward multicast information to downstream devices.

PIM-SM implements unique forwarding trees for each multicast group. These trees are called Rendezvous Point Trees (RPTs) since they rely on a central router called a rendezvous point. After a short period of time, optimized shortest path trees may replace these rendezvous point trees.

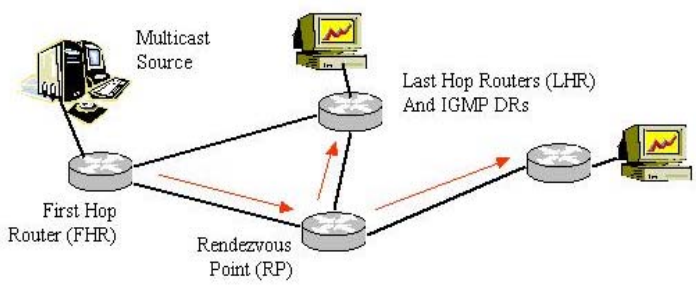
The Role of Rendezvous Points

PIM-SM is a stateful protocol. Routers involved in PIM-SM networks must keep track of the state of various other routers and the multicast distribution trees for all receivers. Stateful information must be maintained for each and every multicast group. This can present severe scalability implications since all routers must dedicate substantial memory and processing resources to these functions.

To offload the majority of the routers, PIM-SM has centralized some of these functions by creating an entity called the rendezvous point (RP). Each multicast group has its own rendezvous point responsible for forwarding information from the source to all registered receivers. In essence, the RP is the root of the rendezvous point trees (RPTs). The rendezvous point is also the most critical test point for PIM-SM functionality and scalability.

Routers configured as candidate RPs announce their presence, along with information about the groups they can service to the bootstrap router (BSR). The BSR is chosen in a separate election and will flood (i.e., multicast) information about all RPs to all active PIM routers. Therefore, when a last hop router (LHR) needs to join a new multicast group, it will be able to notify the appropriate rendezvous point.

The diagram below shows a typical rendezvous point tree (RPT). The multicast source in the upper-left corner of the diagram transmits data to the first hop router (FHR). The FHR knows the location of the RP for that particular group (it learned this information from the bootstrap router). The FHR forwards the data to the RP. The RP will be the root of the rendezvous point tree and distribute the multicast data to all registered receivers.



Verifying PIM-SM Works

PIM-SM testing should focus on the functional, performance and scalability aspects of a PIM-SM router or rendezvous point. From a functional perspective, the tester should verify that all of the basic operations associated with the PIM-SM protocol perform correctly. This process validates the basic multicast functionality of a device — a necessary first step before testing performance or scalability characteristics.

Performance testing typically involves measuring the data-plane performance when packets are replicated. This requires the DUT to transmit multiple packets for every multicast packet received. This is taxing on the CPU, backplane and other ancillary resources of the DUT. Another equally important aspect of performance involves identifying the latency associated with control plane events such as PIM-SM “joins” and “leaves.”

Scalability Concerns

Scalability testing is a major concern for equipment manufacturers, end-users and service providers. Since most router ports will be attached to a LAN switch or hub, they could potentially support hundreds or thousands of users. Each user may, from time to time, subscribe to a unique set of multicast groups. Therefore, the router may be required to track hundreds or even thousands of groups. Rendezvous points for large networks may need to track an even greater quantity of groups. At some point, the router will become saturated, making it critical for equipment manufacturers, service providers and users to identify and understand these limits.

Test Methodologies and Spirent's TeraRouting Tester

PIM-SM functional testing will be the primary focus of this Spirent Communications test methodology journal. The test methodologies serve as examples only; they are not all encompassing multicast routing testing solutions. Most of the examples will not use a concurrent routing protocol or unicast traffic, but such variables can be added to increase test realism.

The first test, RP Functionality, tests the RP's basic functions. The user will validate several aspects of the PIM-SM protocol such as the neighbor discovery process and the processing of PIM "joins."

The second test, Reverse Path Forwarding Check validates the Reverse Path Forwarding (RPF) algorithm of the DUT. This is accomplished by first establishing the DUT can correctly process multicast traffic. Traffic is then introduced with incorrect source addresses. The DUT should detect the induced reverse path violation and not forward this traffic.

Both of the tests included in this journal require at least two SmartBits ports. More extensive testing can be conducted using the same basic methodology with additional ports. Increased port counts are especially useful for performance and scalability tests.

In addition to the SmartBits hardware platform, Spirent Communications' TeraRouting Tester (TRT) software application will be used for both of these tests. TRT allows the user to emulate advanced unicast or multicast network protocols and topologies. Traffic can be sent easily to and from all of these emulated devices and networks. Additionally, negative testing can be accomplished using TRT's capabilities.

In this journal, Gigabit Ethernet ports are used for all test methodologies. However, other media and speeds can be used. Finally, all tests in this journal are based on PIM-SMv4. IPv6 addresses can be directly substituted for the PIM-SMv4 parameters if IPv6 testing is needed.

Making A Difference

There is much to know about testing multicast applications and many steps exist for improving network performance. Spirent believes this journal is a good way to begin because it provides step-by-step testing procedures. While the test methodologies in this journal are a start, Spirent Communications offers extensive support with PIM-SM. If you need more information, let us know how we can assist.

Spirent Communications
www.spirentcom.com

TM-0192

Rendezvous Point Functionality

Associated RFCs

- RFC 2362 Protocol Independent Multicast - Sparse Mode (PIM-SM): Protocol Specification, June 1998
- draft-ietf-pim-sm-v2-new-11 Protocol Independent Multicast - Sparse Mode (PIM-SM): Protocol Specification (Revised), November 2004

Overview

When a downstream router such as a last hop router (LHR) wants to receive multicast traffic for a particular group, it sends PIM-SM “join” messages to the rendezvous point (RP). The RP should add the new router to the appropriate multicast distribution tree, and then forward multicast data to the device.

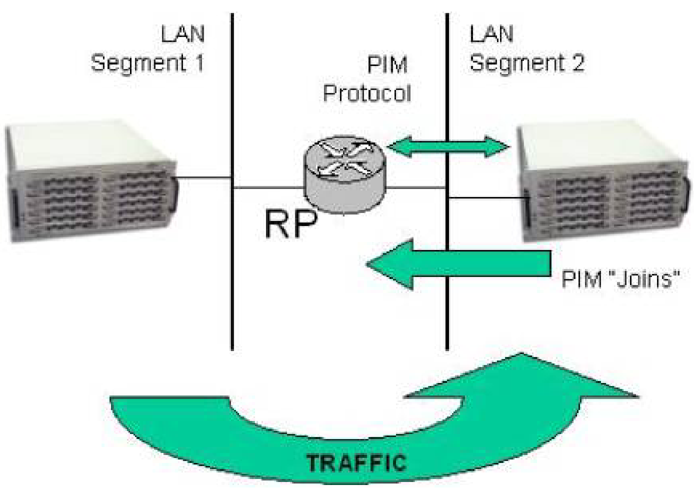
In this test, the device under test (DUT) will be the RP. SmartBits (TRT) Port-2 will be used to emulate an LHR using the PIM-SM protocol. The LHR will join several of the RP’s multicast groups. SmartBits Port-1 will act as an upstream router, generating multicast data streams. The correct behavior of the DUT will consist of properly implementing and utilizing the PIM-SM protocol, adding the LHR to the appropriate multicast distribution trees, and then forwarding traffic for the correct multicast groups.

Objective

This test will validate the DUT's basic PIM-SM protocol functionality, including the rendezvous point (RP) operations. It validates RP functionality, the processing of PIM “join” requests and traffic forwarding.

Setup

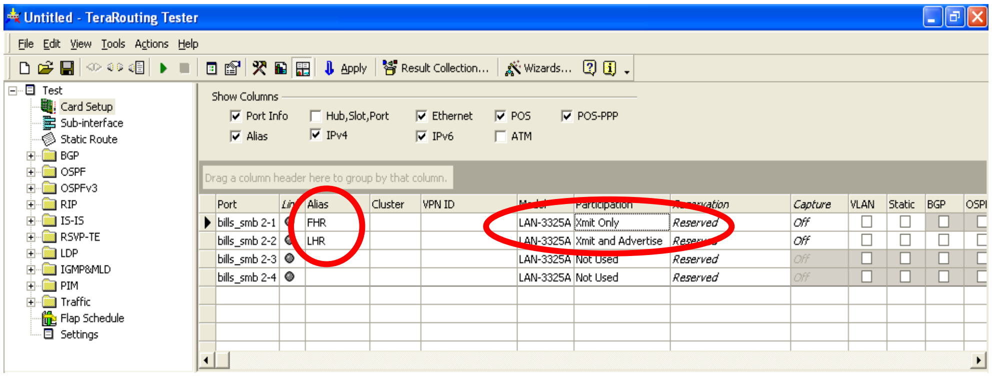
The basic test setup is indicated in the diagram below. VLANs will be used on LAN segment 2 in order to simulate multiple receivers for the same multicast groups.



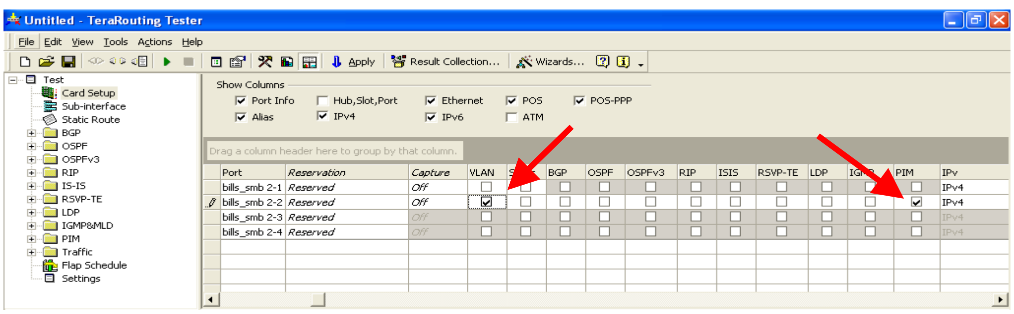
Step-by-Step Testing

1. Configure the local router to support PIM-SM. (This test will use VLANs in order to conserve physical ports and further stress the DUT, but the test can also be conducted without them. VLAN information must also be configured in the DUT.)

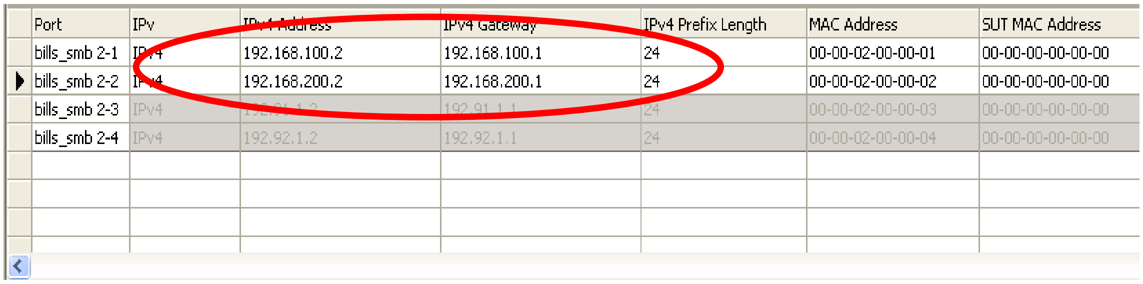
2. Select the proper SmartBits ports. Set Port-1 to "Xmit Only" and set Port-2 to "Advertise Only" or "Xmit and Advertise." Add aliases if desired. Reserve the ports after they have been configured.



3. Enable VLANs and PIM on Port-2. Disable RIP (which is enabled by default) for Port-2.



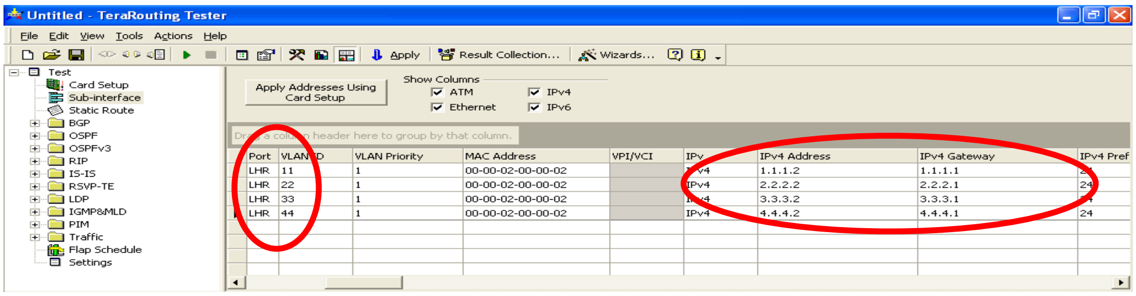
4. Configure the correct addresses for the tester and the DUT.



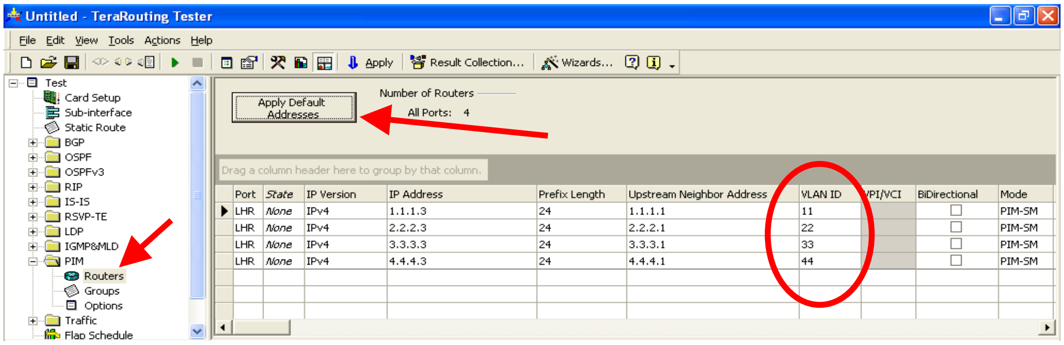
Port	IPv	IPv4 Address	IPv4 Gateway	IPv4 Prefix Length	MAC Address	SUT MAC Address
bills_smb 2-1	IPv4	192.168.100.2	192.168.100.1	24	00-00-02-00-00-01	00-00-00-00-00-00
bills_smb 2-2	IPv4	192.168.200.2	192.168.200.1	24	00-00-02-00-00-02	00-00-00-00-00-00
bills_smb 2-3	IPv4	192.91.1.2	192.91.1.1	24	00-00-02-00-00-03	00-00-00-00-00-00
bills_smb 2-4	IPv4	192.92.1.2	192.92.1.1	24	00-00-02-00-00-04	00-00-00-00-00-00

5. Click on the “Sub-Interface” icon. This will take you to the VLAN configuration screen. Add three new lines so that a total of four VLANs/LHRs will be emulated.

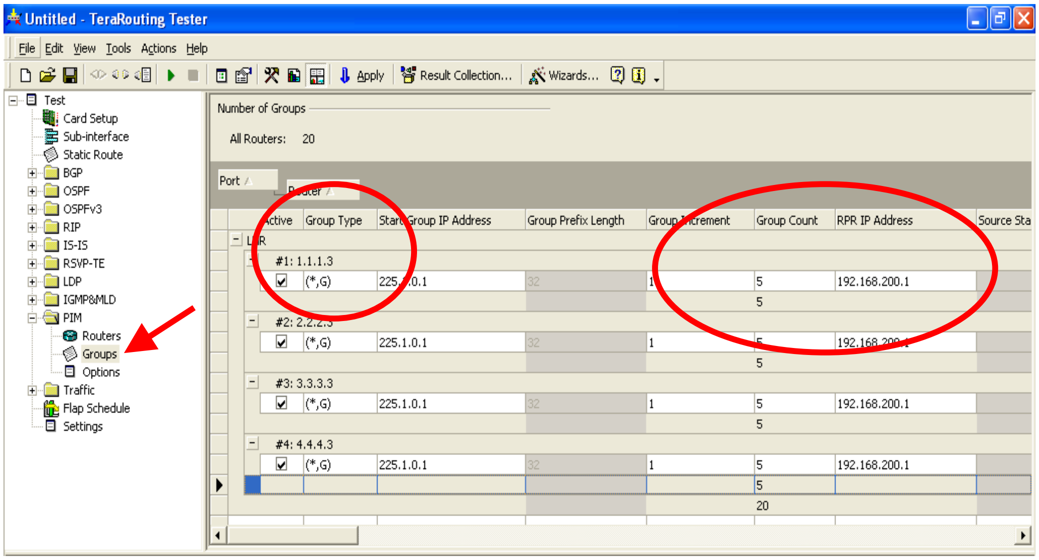
6. Configure the correct VLAN-IDs and IP addresses for the tester and the gateway (DUT).



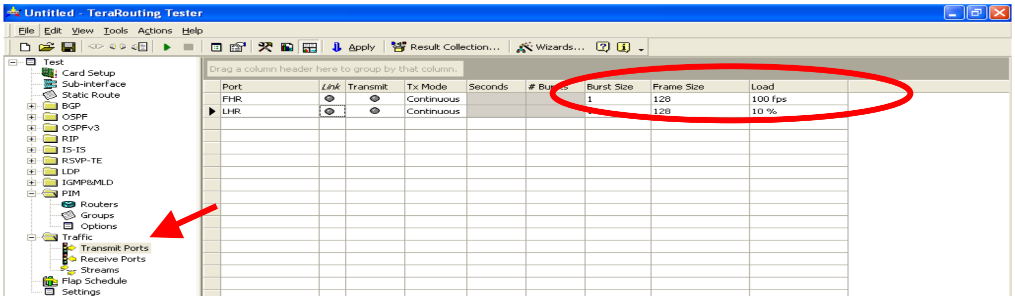
7. Select “PIM Routers” from the navigation window. Right-click to add three more lines. Fill-in the correct VLAN-IDs, then click on the button for “Apply Default Addresses” to automatically fill in appropriate IP addresses for each emulated router.



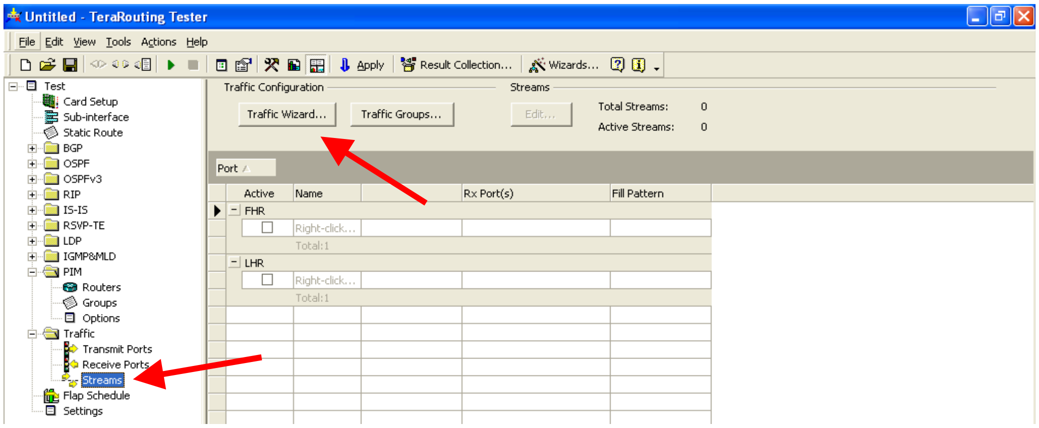
8. Select “PIM Groups” from the navigation window. Right click on each line to add groups. Use the default group type (*,G). Select the quantity of groups to be joined by each emulated LHR. In this case, each router will join the same five groups. Fill in the address of the RP.



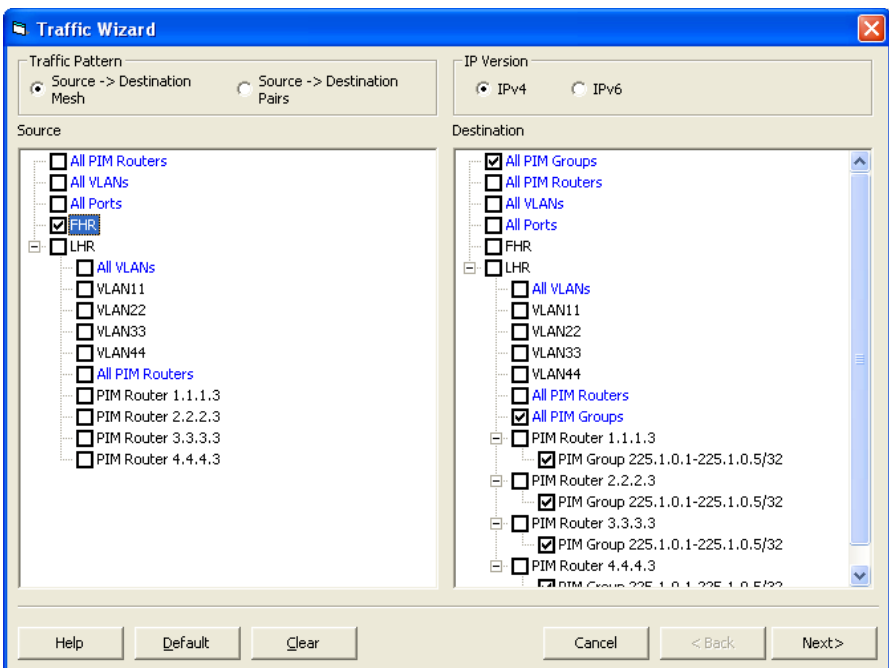
9. From the “Traffic - Transmit Ports” menu, select the appropriate frame size and loading parameters. In this example, 128-byte packets will be transmitted from Port-1 at a constant rate of 100 frames per second. No packets will be transmitted from Port-2 (the LHR) so no further configuration is necessary for that port.



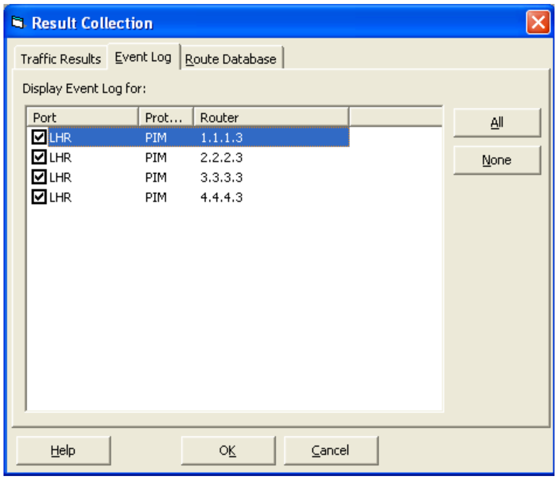
10. From the navigation window, select "Streams." Then select the "Traffic Wizard."



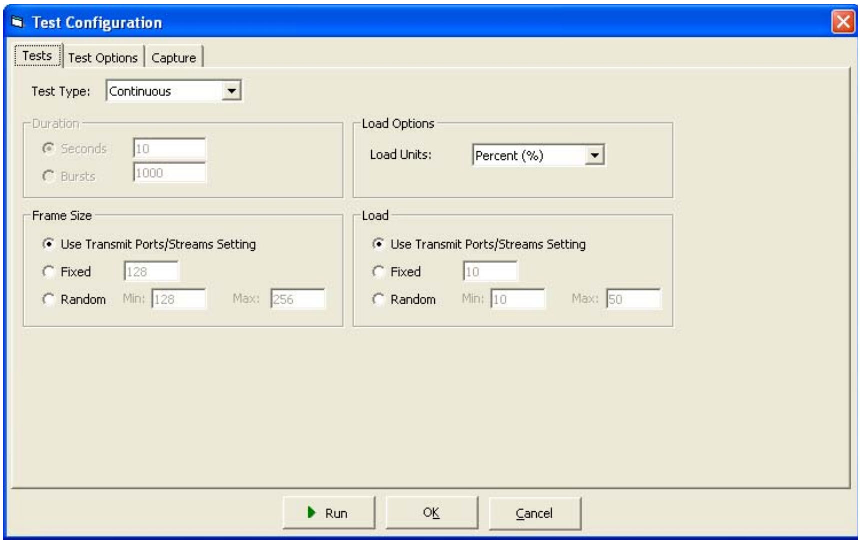
11. On the left-hand side of the wizard, select the FHR as the source for all transmissions. On the right-hand side, check the box for "All PIM Groups" as the destination. Accept the remainder of the defaults for the traffic wizard. After running the wizard, a single traffic stream will be constructed.



12. Select the "Results Collection" button on the upper part of the configuration screen. Click on the "Event Log" tab. Enable event logging by checking the four boxes next to the emulated LHRs. This will be a valuable tool for debugging any potential problems.



13. Click on the green arrow to run the test. Accept the default settings for remaining fields in the Test Configuration menu.



14. Validate the PIM neighbor states. From the DUT, verify that all four neighbors are active.

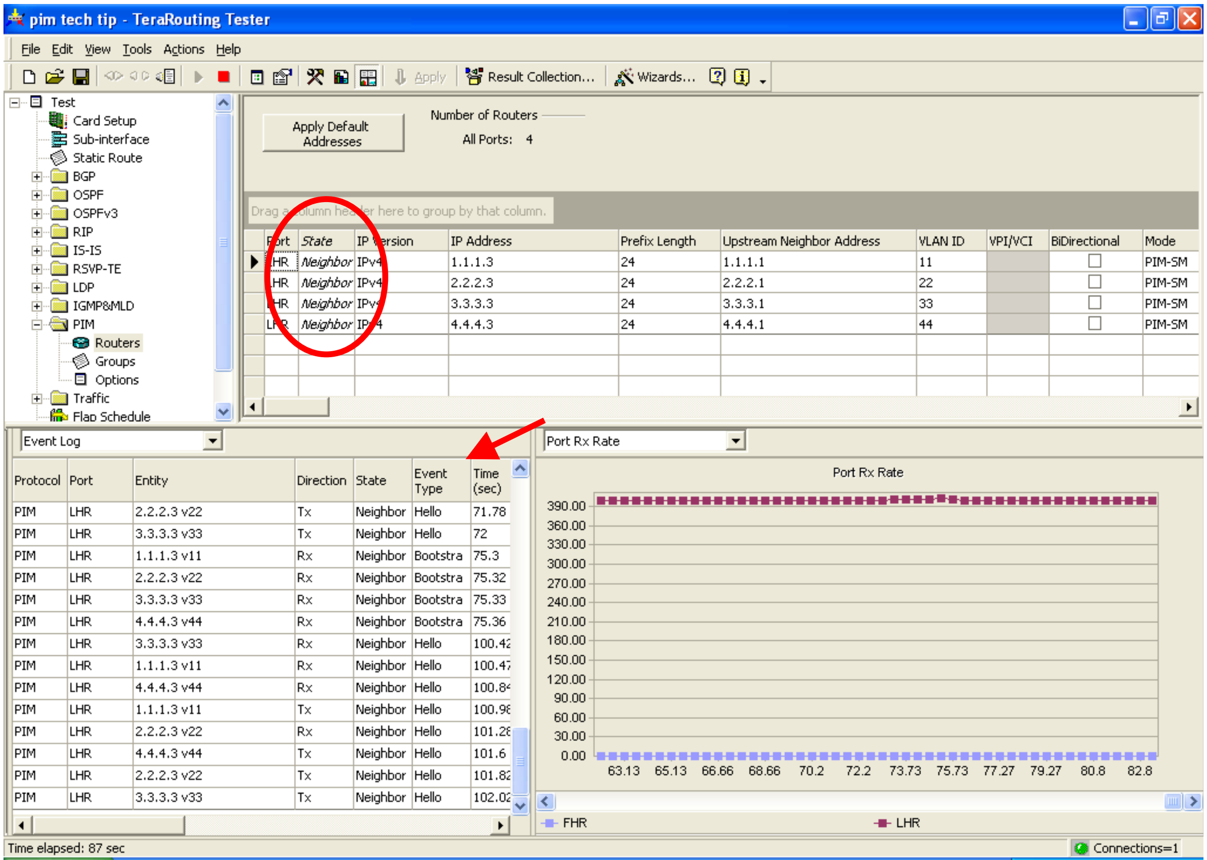
PIM Neighbor Table

Neighbor Address	Interface	Sample DUT Table	Priority/Mode
1.1.1.3	FastEthernet0.1	00:00:08/00:01:36 v2	1 / DR
2.2.2.3	FastEthernet0.2	00:00:08/00:01:36 v2	1 / DR
3.3.3.3	FastEthernet0.3	00:00:07/00:01:37 v2	1 / DR
4.4.4.3	FastEthernet0.4	00:00:08/00:01:36 v2	1 / DR

15. From the DUT's console port, also verify the status of the five requested multicast groups.

Group: 225.1.0.1, RP: 192.168.200.1, v2, next RP-reachable in 00:01:13
Group: 225.1.0.2, RP: 192.168.200.1, v2, next RP-reachable in 00:01:13
Group: 225.1.0.3, RP: 192.168.200.1, v2, next RP-reachable in 00:01:13
Group: 225.1.0.4, RP: 192.168.200.1, v2, next RP-reachable in 00:01:13
Group: 225.1.0.5, RP: 192.168.200.1, v2, next RP-reachable in 00:01:13

16. Also validate the PIM neighbor status from the SmartBits Tester's perspective. The "PIM Routers" configuration window will indicate the current neighbor state. The Event Log (lower left) will also display the protocol interaction between the router and the tester.



17. Validate the receive rate for the multicast data streams. In the example used in this test, a stream of 100 frames per second should be delivered to four different LHRs, each on its own VLAN. Accordingly, the tester expects to receive 400 frames per second on Port-2. The graph in the lower-left corner of the above diagram indicates that the receive rate is correct.

18. In order to further test the functionality of the PIM-SM rendezvous point, this test should be rerun modifying some or all of the parameters listed below. Most of these parameters can be modified interactively, while the test is running. This form of interactive testing will provide the user with real-time responses to these dynamic changes:

    a. Group quantities

    b. Use non-contiguous groups

    c. Modify the PIM timers and counters

    d. Port and/or VLAN quantities

    e. Traffic profiles (frame sizes and rates)

    f. Introduce background traffic

    g. Alternate PIM "join" and "prune" messages

    h. Modify PIM message delays and "packed" selections ("PIM Options" window)

TM-0193

Reverse Path Forwarding Check

Associated RFCs

- RFC 2362 Protocol Independent Multicast - Sparse Mode (PIM-SM): Protocol Specification, June 1998
- draft-ietf-pim-sm-v2-new-11 Protocol Independent Multicast - Sparse Mode (PIM-SM): Protocol Specification (Revised), November 2004

Overview

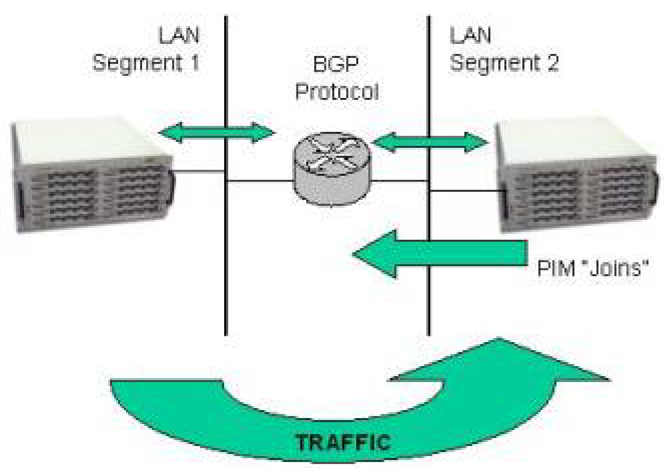
Unicast routers forward packets to their destination. Multicast routers operate based upon an opposite principle – they forward packets away from their sources. While this may seem like a rather subtle distinction, this paradigm known as reverse path forwarding is an absolutely critical part of multicast routing.

Routers build multicast distribution trees for each multicast group. As the quantity of receivers increases, these trees can become extremely complex. The propensity for routing loops increases along with this complexity – especially as multiple users join and leave the groups. Reverse Path Forwarding is the loop avoidance mechanism invoked by most multicast routing implementations.

When a multicast router receives a multicast datagram, it reads the source address contained in the packet. (The destination address will be a Class-D IP address for a multicast group.) The router uses its existing unicast routing table to lookup the source address. Then it determines which interface would be used to forward a unicast packet to that particular source address. If the packet arrived on that interface, then it is considered to be a valid packet, and it will be forwarded to the downstream routers (e.g. away from the source). If the packet arrived on a different interface, it is presumed that it has been routed incorrectly or possibly created a loop condition, so it is discarded.

Testing the RPF check functionality will require the use of a unicast routing protocol. In this particular test, BGP4 will be used. After verifying that the DUT is correctly processing multicast packets and protocols, a new stream will be injected that intentionally violates the RPF check. This stream should not be forwarded to the downstream routers.

The first step is to create a functioning multicast and BGP emulated network as shown below.

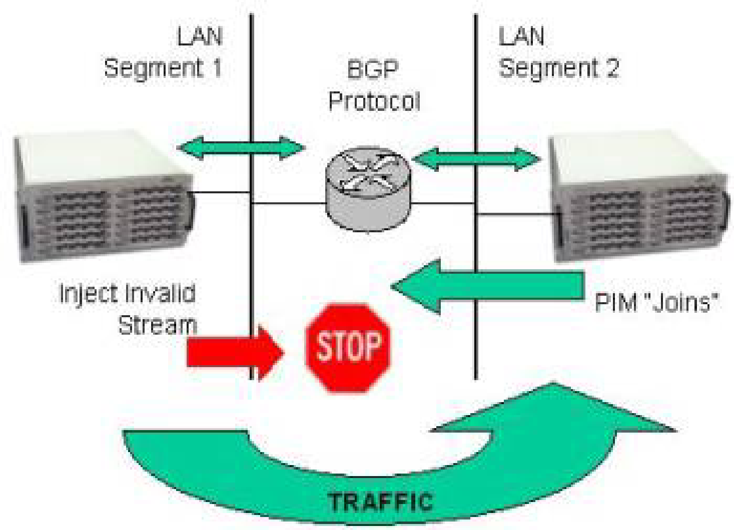


This test validates a router's ability to update its forwarding tables and terminate one or more workstations from the multicast group. IGMP Version 3 is used.

Objective

This test validates the DUT's Reverse Path Forwarding check by generating a traffic stream that violates this condition. This stream should not be forwarded to the specified multicast group.

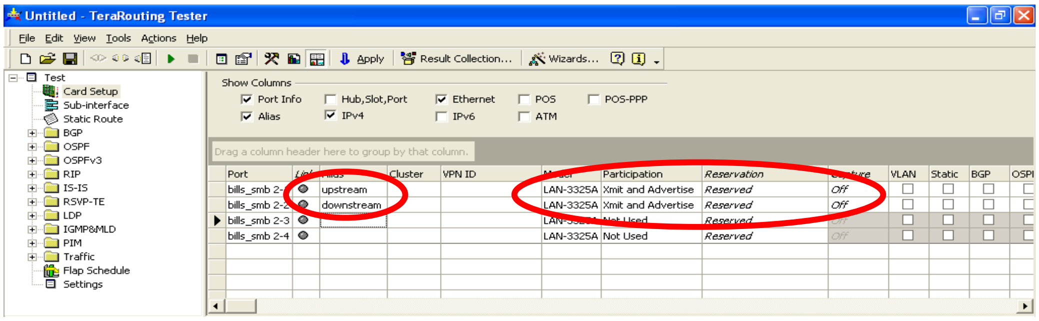
Setup



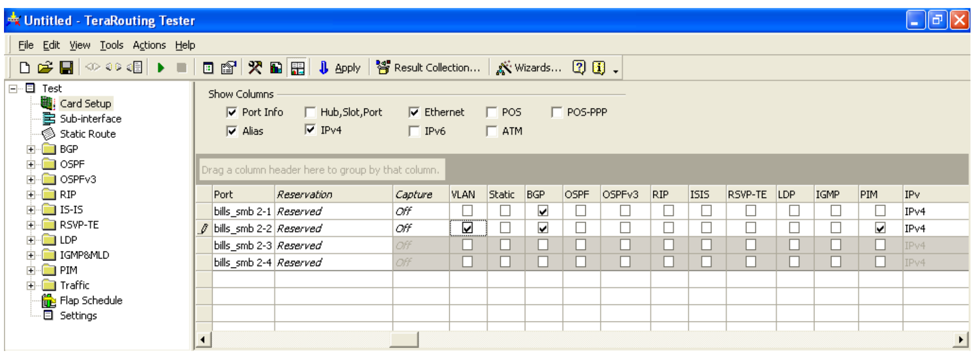
Step-By-Step Testing

1. Configure the local router to support PIM-SM and BGP. Be sure to include the correct IP address and AS-Numbers for the tester. (This test will use VLANs in order to conserve physical ports and further stress the DUT, but the test can also be conducted without them. VLAN information must also be configured in the DUT.)

2. Select the proper SmartBits ports. Set both ports to “Xmit and Advertise” Add aliases if desired. Reserve the ports after they have been configured..)



3. Disable RIP for both ports (this is always enabled by default). Enable BGP for both ports. Enable PIM for Port-2 (the “downstream” port). Enable VLANs for Port-2 to simulate several multicast ports.

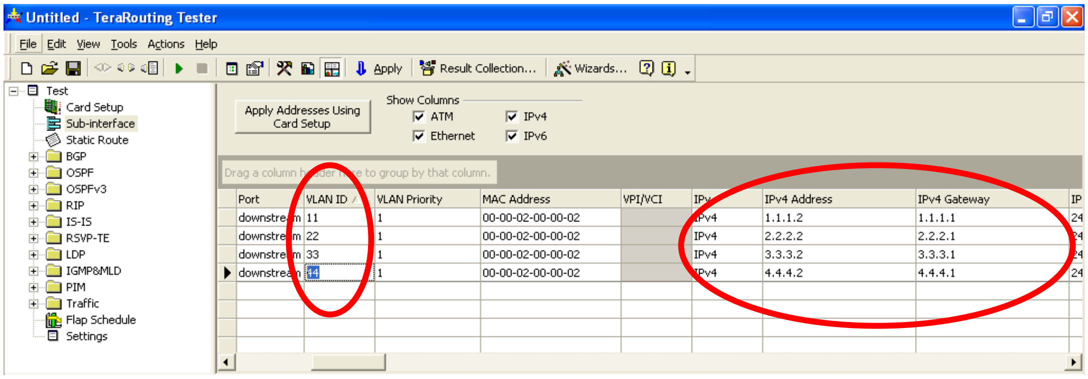


4. Configure the correct addresses for the tester and the DUT.

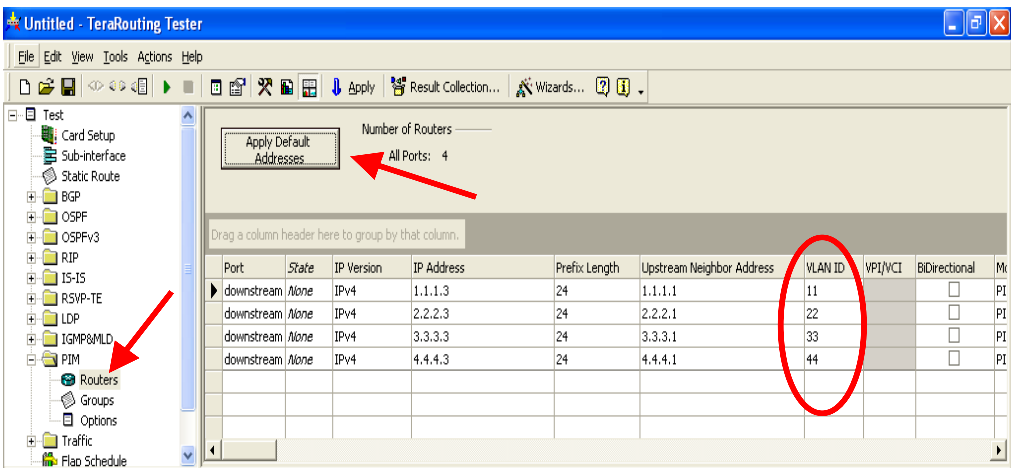
Port	IPv	IPv4 Address	IPv4 Gateway	IPv4 Prefix Length	MAC Address	SUT MAC Address	MTU
bills_smb 2-1	IPv4	192.168.100.2	192.168.100.1	24	00-00-02-00-00-01	00-00-00-00-00-00	1500
bills_smb 2-2	IPv4	192.168.200.2	192.168.200.1	24	00-00-02-00-00-02	00-00-00-00-00-00	1500
bills_smb 2-3	IPv4	192.91.1.2	192.91.1.1	24	00-00-02-00-00-03	00-00-00-00-00-00	1500
bills_smb 2-4	IPv4	192.92.1.2	192.92.1.1	24	00-00-02-00-00-04	00-00-00-00-00-00	1500

5. Click on the “Sub-Interface” icon. This will take you to the VLAN configuration screen. Add three new lines so that a total of four VLANs/LHRs will be emulated.

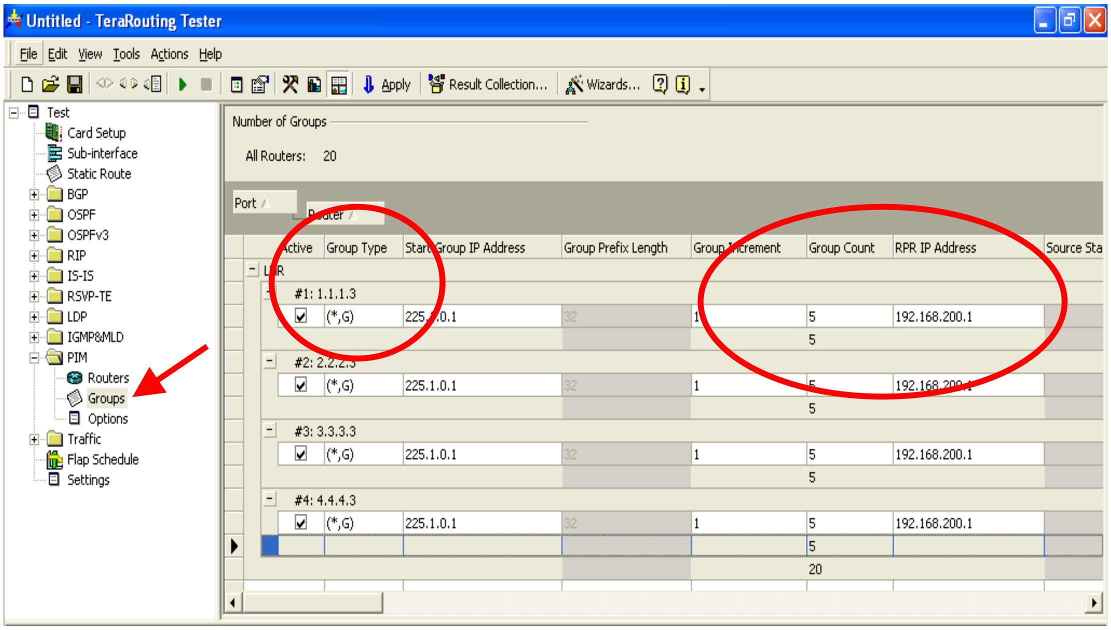
6. Configure the correct VLAN IDs and IP addresses for the tester and the gateway (DUT).



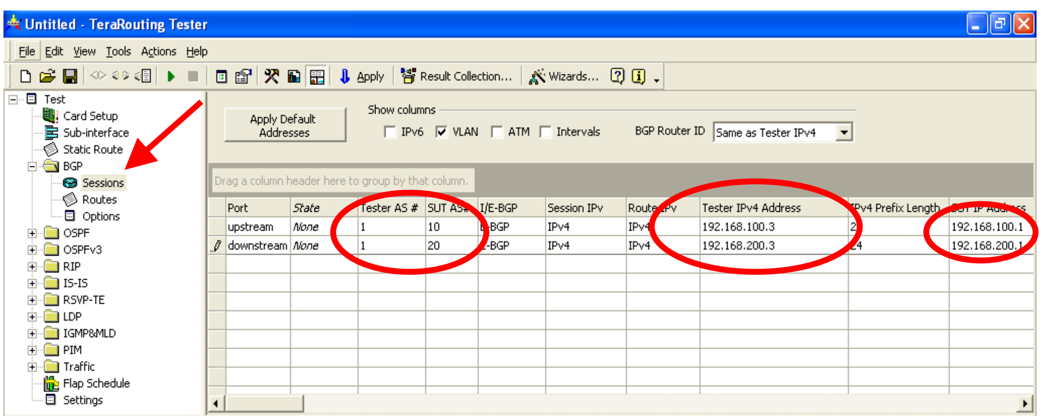
7. Select "PIM Routers" from the navigation window. Right-click to add three more lines. Fill in the correct VLAN IDs, then click on the button for "Apply Default Addresses." This will automatically fill in the appropriate IP addresses for each emulated router.



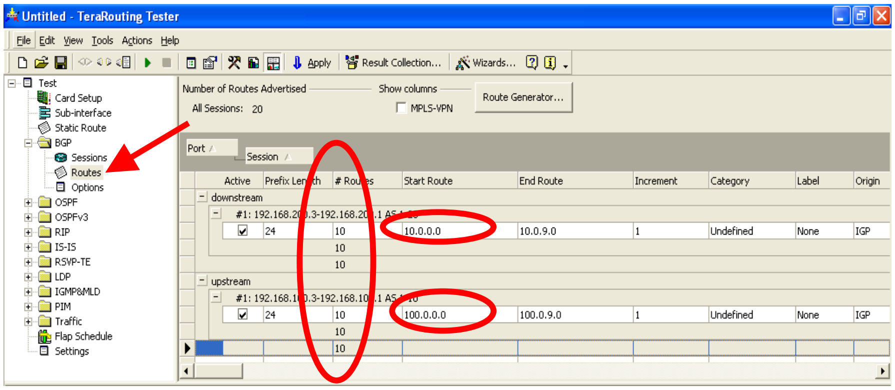
8. Select "PIM Groups" from the navigation window. Right-click on each line to add groups. Use the default group type (*,G). Select the quantity of groups to be joined by each emulated LHR. In this case, each router will join the same five groups. Fill in the address of the DUT which will act as the RP.



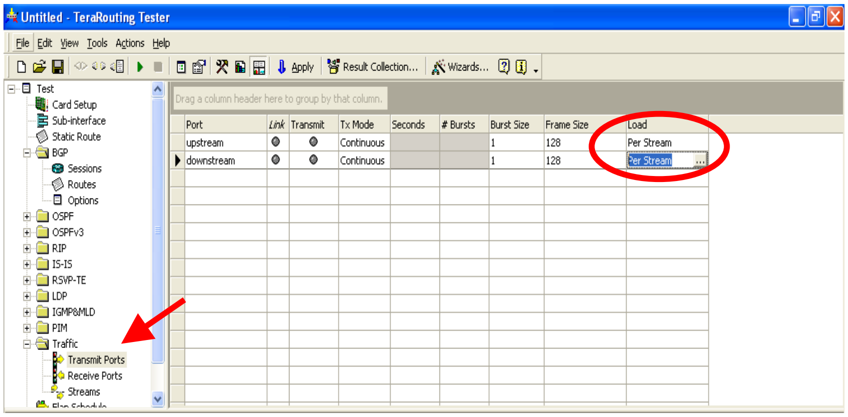
9. Use the navigation window to select BGP Sessions. Configure the correct Autonomous Systems Numbers and IP Addresses for the tester and the DUT. Note that these must match the configuration of the DUT. Also note that in this particular example, VLANs are not necessary for the BGP portion of the configuration.



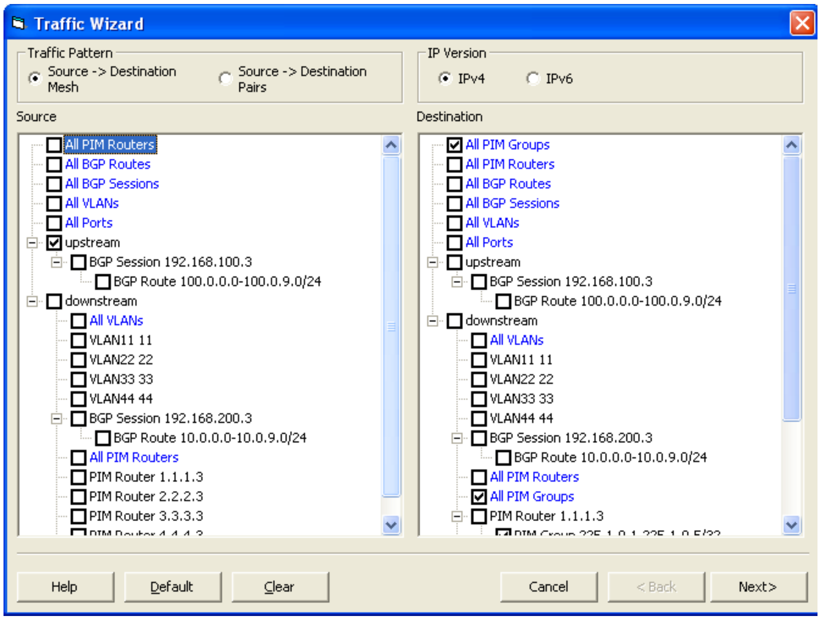
10. Select BGP Routes from the navigation window. Add ten routes (or any other desired quantity) to each emulated router. Make sure the routes use distinct (and hopefully easily distinguishable) addresses. In the example below, the downstream route block starts at 10.0.0.0 and the upstream block begins with 100.0.0.0.



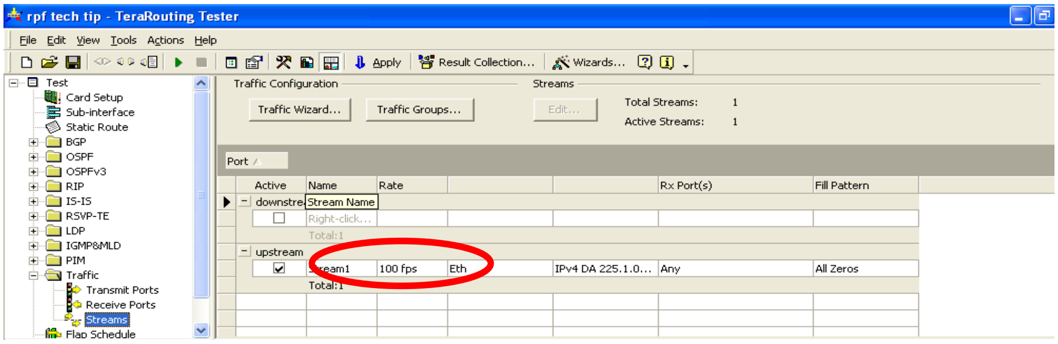
11. Go to Traffic → Transmit Ports. Change the “Load” value to read “Per Stream” so that unique traffic loads can be created for each data stream.



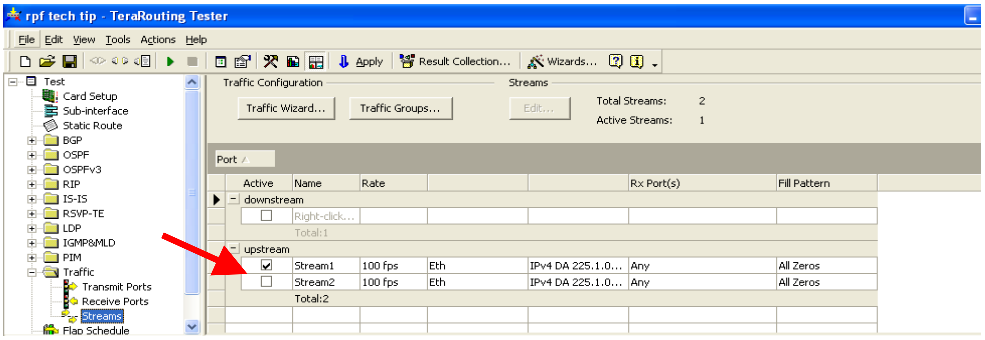
12. Select Traffic → Streams, then click on the button for the traffic wizard. On the left-hand (source) side of the traffic wizard screen, only select the upstream port as the source. On the right-hand side, select "All PIM Groups" as the destination. The remaining defaults can be accepted.



13. A single stream should have been created. Set the rate to 100 frames per second.



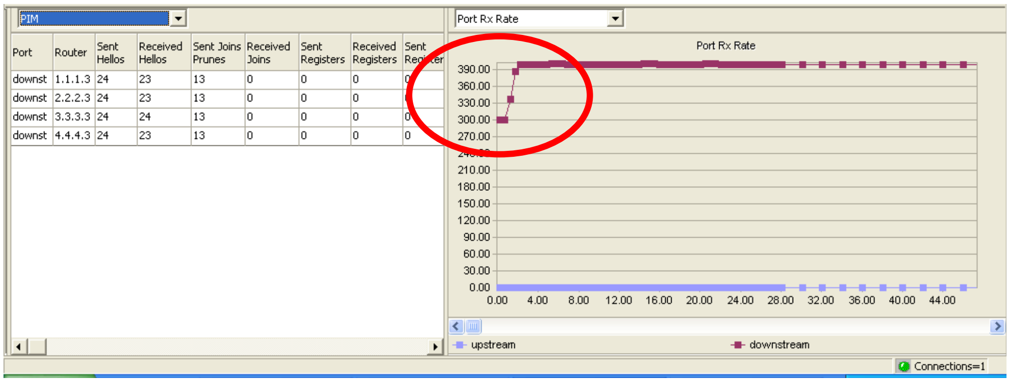
14. Right-click to copy and paste a second identical stream below the first. Rename this second stream to "Stream 2" and deactivate it by deselecting the "Active" button.



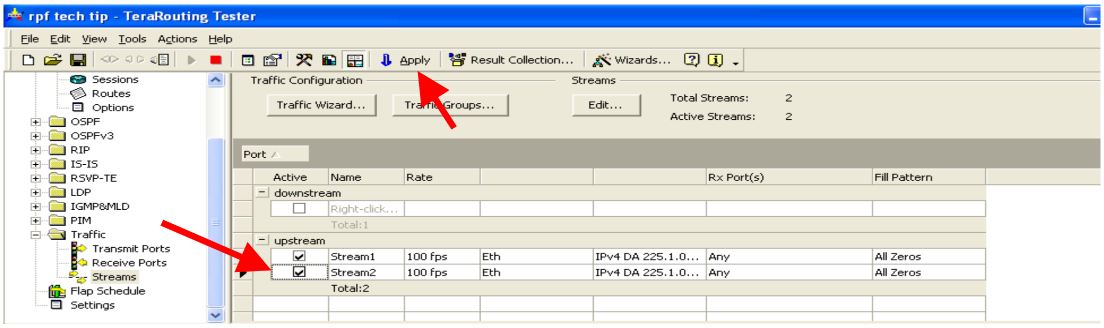
15. Start the test. Use the Green Arrow to begin running the test, and accept the default values for all other parameters.

16. Systematically verify that the links are up (solid green lights on the Card Setup window), the BGP sessions are established and the PIM neighbors have been correctly activated. Check the DUT's stateful data to confirm this information. Also validate the existence of five groups in the PIM RP Group Table and check the BGP route table (it should contain both 100.0.0.0 routes and 10.0.0.0 routes).

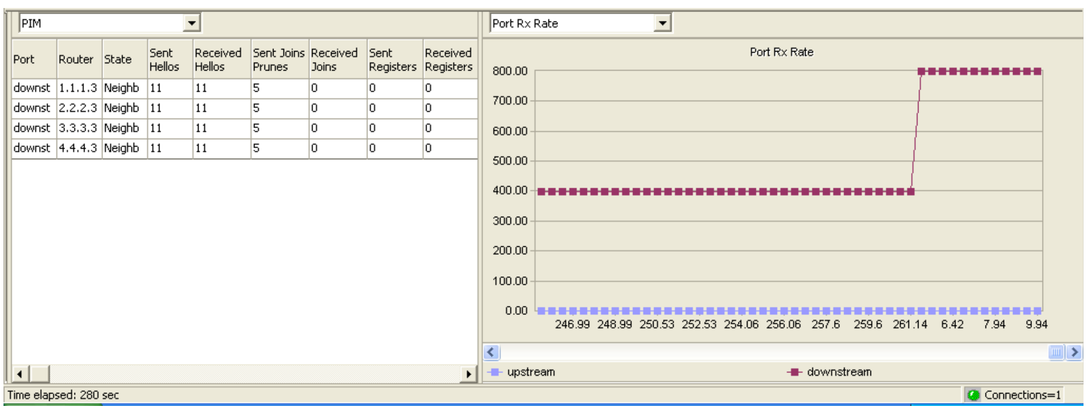
17. The traffic is being generated at a rate of 100 frames per second. Since this traffic is being replicated by the router for four different VLANs, each of which is a member of every multicast group, the expected receive rate is 400 frames per second. Verify this rate.



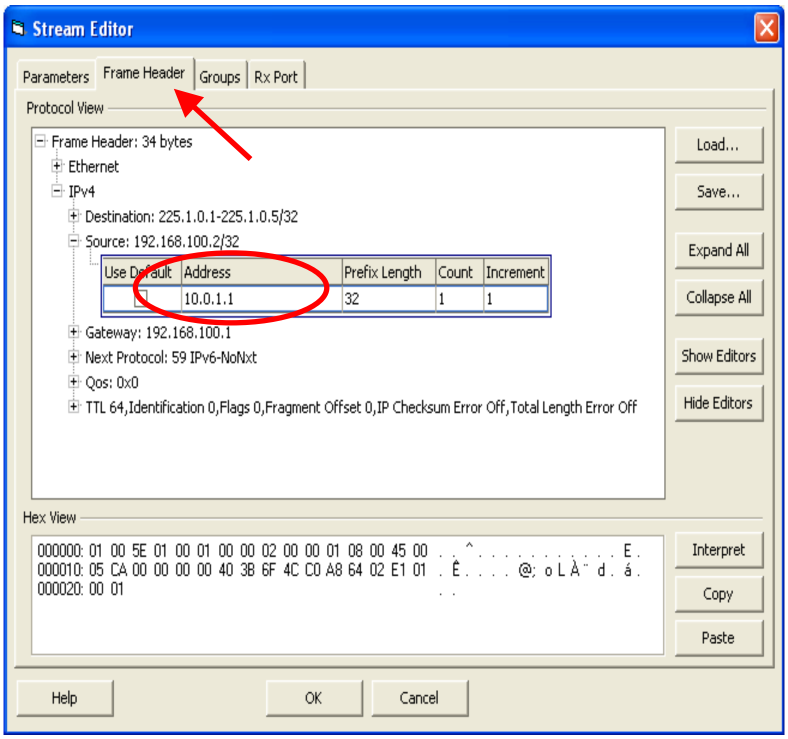
18. While the test is running, activate the second stream. This can be accomplished interactively by checking the “Active” box and then clicking on the “Apply” button.



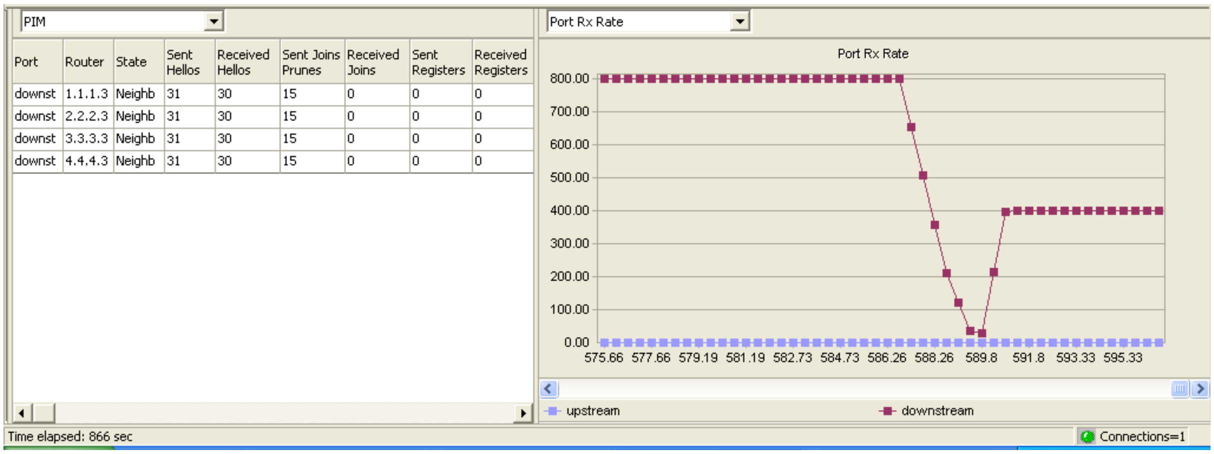
19. Since the second stream is identical to the first stream, the traffic rate has effectively been doubled. Therefore, the receive rate should also double, increasing from 400 frames per second to 800 frames per second.



20. The next step is to modify the second stream to use an invalid source address, and therefore trigger an RPF violation. Select the second stream from the streams window and click on the "Edit Stream" button. This will invoke the stream editor. Go to the "Frame Header" tab. Modify the source address to be 10.0.1.1, an address that was advertised by BGP on Port-2. Since the stream originates on Port-1, this address should not be accepted by the DUT. After completing this modification, click on the "Apply" button for it to take affect.



21. The second stream contains an invalid source address, so the packets should be dropped instead of forwarded. If this function is operating correctly, the throughput should be reduced back to the original rate of 400 frames per second.



Port	Router	State	Sent Hellos	Received Hellos	Sent Joins Prunes	Received Joins	Sent Registers	Received Registers
downst	1.1.1.3	Neighb	31	30	15	0	0	0
downst	2.2.2.3	Neighb	31	30	15	0	0	0
downst	3.3.3.3	Neighb	31	30	15	0	0	0
downst	4.4.4.3	Neighb	31	30	15	0	0	0

22. This test can be repeated while modifying any of the following parameters:
    a. Port and/or VLAN quantities
    b. Multicast group quantities
    c. Unicast routing protocols
    d. Unicast route quantities
    e. Traffic rates
    f. Introduction of background unicast traffic

Glossary

This glossary provides definitions of the terminology, abbreviations, and acronyms used in this Spirent Communications test methodology journal as well as terms based on telecom technology and standards.

Address Resolution Protocol (ARP).

The means by which a physical MAC address is associated with a particular IP address.

Autonomous System (AS).

A group of networks within a common administrative domain. Typically, these networks will share a common interior gateway routing protocol.

Border Gateway Protocol (BGP).

The means by which a physical MAC address is associated with a particular IP address.

Bidir-PIM.

A proposed IETF draft for bi-directional multicast communications.

Bootstrap Messages.

Messages generated by the bootstrap router. These messages are multicast to all PIM routers to provide them the identities of the rendezvous point (RP) routers for all available multicast groups.

Bootstrap Router (BSR).

A router used by the PIM-SM protocol to disseminate information.

Broadcast.

A method for transmitting data to every user of a particular network or segment.

Class-D Address.

IP addresses in the range 224.0.0.0 - 239.255.255.255. This range has been specifically dedicated for multicast communications.

Designated Router (DR).

This term is used in several routing protocols, each of which has its own specific purpose for the DR. IGMP and MLD elect a DR when multiple routers are connected to a single LAN segment. The DR handles all of the multicast registration requirements for that particular segment.

Distance Vector Multicast Routing Protocol (DVMRP).

An early multicast routing protocol like RIP.

First Hop Router (FHR).

The router at the beginning of the communications path for multicast messages. Typically, this will be the default gateway for the source computer.

Format Prefix.

The first three bits of an IPv6 address indicates the overall format of the address. (Unicast and multicast formats are supported.)

Internet Assigned Number Authority (ANA).

The controlling body for public IP addresses.

Internet Control Message Protocol (ICMP) (RFC 792).

Used for reporting errors and troubleshooting IP networks.

Internet Engineering Task Force (IETF).

The "standards body" of the Internet. All RFCs come from IETF.

Internet Group Management Protocol (IGMP).

An extension of the Internet Protocol (IP) used by end stations to register with multicast groups.

IGMP Snooping.

A method employed by some Layer 2 switches to determine the multicast group membership of their locally attached workstations. The switches do not participate in the IGMP process; they just passively read the packets that are transmitted to/from the workstations and the local router.

Last Hop Router (LHR).

The router at the end of the delivery path for multicast messages. This router sends the messages to the receivers based upon their IGMP or MLD registration.

Multicast.

A communication transmission from a single sender to a unique group of multiple receivers.

Multicast Listener Discovery (MLD).

An IPv6 version of IGMP for registering IPv6 workstations with multicast groups.

Multicast OSPF (MOSPF).

Provides the extensions to OSPFv2 to support multicast communications.

Open Shortest Path First (OSPF).

An interior gateway protocol that uses link-state or Dijkstra calculations to determine the optimal path to a given destination. This is a popular protocol for large private networks.

Protocol Independent Multicast (PIM).

A multicast forwarding protocol that uses the routers' existing routing tables (derived from other protocols) to forward traffic.

PIM Dense Mode (PIM-DM).

A version of PIM that uses a "push" methodology to deliver multicast traffic to densely populated user communities.

PIM Sparse Mode (PIM-SM).

A commonly used version of PIM that relies on "pull" methodologies to deliver multicast traffic. A downstream user must specifically request a multicast traffic stream to receive the data.

PIM Source Specific Mode (PIM-SSM).

A version of PIM in which the source dictates the forwarding tree to all of the destinations.

Prune.

A message used by downstream multicast routers to inform upstream routers that they want to withdraw from a particular multicast group.

Rendezvous Point (RP).

A central router used by PIM-SM that will receive all of the traffic from multicast sources and then forward that traffic to the receivers.

Rendezvous Point Trees (RPT).

A multicast forwarding tree for PIM-SM that uses a rendezvous point router.

Reverse Path Tree.

A multicast forwarding tree that routes the data away from the source's location.

Routing Information Protocol (RIP).

An interior gateway protocol for routing data. RIP is based on hop-counts and is a distance-vector protocol.

Shortest Path Tree (SPT).

A direct tree from the multicast source to the receiver(s). This does not use a rendezvous point.

Transmission Control Protocol (TCP).

A connection-oriented transport (Layer 4) protocol used to ensure the reliable delivery of datagrams.

User Datagram Protocol (UDP).

A connectionless transport (Layer 4) protocol. UDP does not facilitate datagram acknowledgements or retransmissions.

Unicast.

A method for transmitting data to one specific end-user or workstation.

Spirent Communications Test Methodologies Information

Spirent Communications at <www.spirentcom.com> has a library of test methodology journals that offer you insight into testing a variety of technologies.

This issue of the Spirent Communications Step-by-Step Test Methodologies journal uses the TeraRouting Tester (TRT) on the SmartBits platform.

The following platform-specific journals can be found on Spirent's Customer Service Center (CSC) at <http://support.spirentcom.com>. Registration is required.

- TRT Edition: High Availability Routing
- TRT Edition: IGMP/MLD Functional Testing
- TRT Edition: Protocol Independent Multicast (PIM)

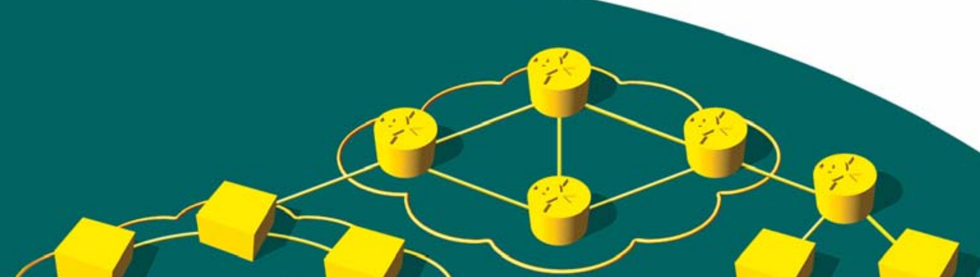
While this journal is platform-specific for TRT, Spirent also provides a downloadable series of generic and informative test methodology journals at <www.spirentcom.com/tmj>:

- Router Performance Edition
- Volume II - Wireless, Edge Router, Metro Optical, VoIP, SS7, QoS and IPv6
- IPv6 Edition
- Multicast Edition
- PPPoX Edition
- Optical Edition
- Edge Router Edition
- MPLS Edition
- IPSec Edition
- Layer 4-7 Edition

Sales and technical support phone numbers are listed on the front inside cover of this journal in case you would like to contact us.

SPIRENT Communications

Analyze | Assure | Accelerate™



P/N 340-5120-001 REV A