MPLS 2011 Public Interoperability Test Results

MPLS Transport Profile, Next-Gen Multicast VPNs

MPLS Services over 100 Gigagbit Ethernet and G.8032

MPLS 2011, similar to its predecessors, will offer its delegates an exclusive opportunity to witness the state of the art networking technologies in an independent setting. Isocore once again built a comprehensive test bed validating the interoperability of leading vendors, and the co-existence of multiple technologies across a common network infrastructure. MPLS 2011 offers a perfect public platform for the delegates to witness the results of a first-ever multi-vendor standards-based MPLS Transport Profile (MPLS-TP) interoperability testing. MPLS-TP testing will showcase statically provisioned Label Switched Paths (LSP) with protection switching, Ethernet service delivery over static pseudowires (PWs), MPLS-TP OAM including BFD connectivity check (CC) and LSP ping for on-demand connection verification (CV). Additionally MPLS-TP LSPs were also tested with ITU-T recommendation Y.1731 based OAM including CC and delay measurement. Isocore showcased the results of the multicast VPNs and G.8032 – Ethernet Ring Protection Switching (ERPS) and MPLS services and Ethernet OAM over 100 Gigabit Ethernet interface.

The testing referenced a compilation of individual tests extracted from Isocore's library of test plans. Isocore primarily focuses on technologies that are standardized by various standard development organizations, such as IEEE, IETF, ITU-T and others.

For the Fall leading edge code (LEC), a weeklong test event was scheduled at Isocore's headquarters in Washington metro area during the week of September 19, 2011. Figure 1 illustrates various technology areas that were included within the scope of the Fall LEC event, and the results obtained were presented at the public demo.

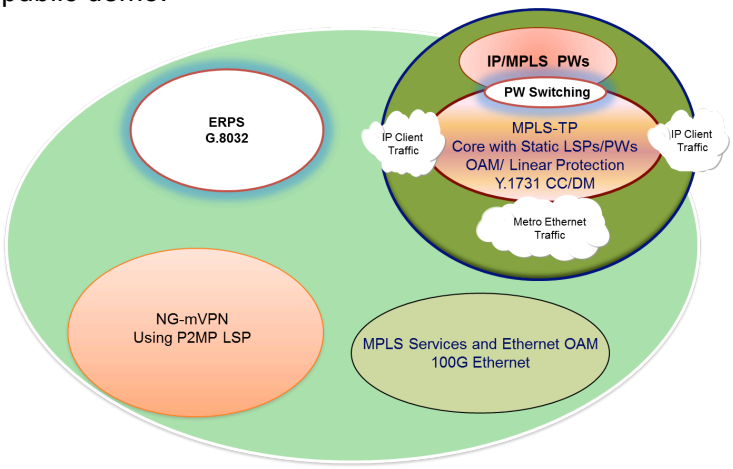

Figure 1: The technologies considered

The Fall LEC testing saw participation from major network equipment manufacturers and test equipment vendors that worked toward a goal of achieving interoperability in various technology areas while building a multi-vendor network.

This white paper presents a high-level overview of what was tested. For some test areas, results from Isocore spring LEC event are also presented to demonstrate the evolving implementations as standards become stable, MPLS-TP being one of the classic examples.

Figure 2 shows the comprehensive setup highlighting the roles played by all participating nodes and logical representation of the network physical topology.

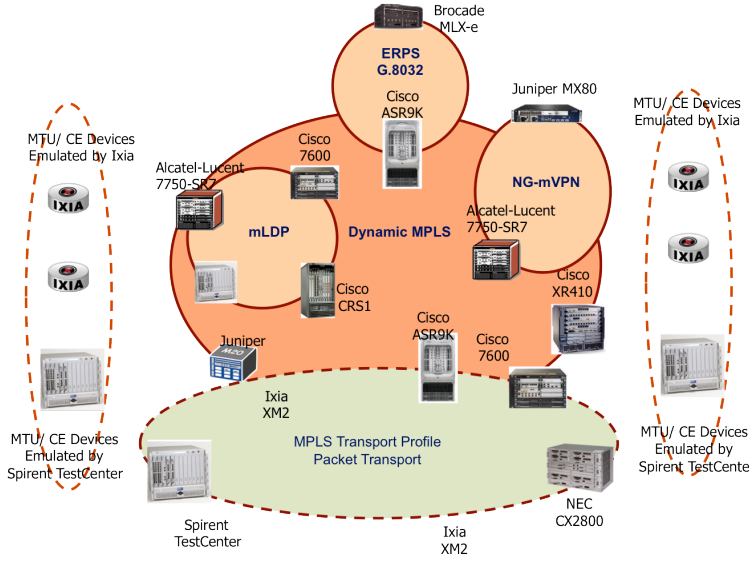

Figure 2: Logical Representation of MPLS2011 Demo Network

During the initial stages of planning for the Fall LEC testing demonstration, several technologies were proposed through the feedback received from participants. Ranking these topics in the order of priority lead to the short list of the following areas, forming the core of the MPLS 2011 Interoperability demonstration.

1. *Standard-based MPLS Transport Profile*
   a. *Statically provisioned co-routed LSPs*
   b. *Linear Protection*
   c. *MPLS-TP OAM - including BFD connectivity Check (CC) and LSP Ping using ACH*
   d. *Y.1731 based OAM*
2. *BGP based multicast VPN (BGP-mVPN)*
3. *MPLS services over 100G connections*
4. *Ethernet Ring Protection (G.8032)*

The Isocore IP/MPLS test network started with a flat network with one autonomous system to give vendors an opportunity to test with each other. The network was subsequently split into different sections focusing on different technologies listed above. This helped to manage different testing objectives efficiently and give vendors the opportunity to continue to focus on their priorities. Figure 2 also illustrates the final integrated testbed at the conclusion of the Fall LEC testing.

Similar to earlier events, Fall 2011 LEC event offered a perfect staging platform for MPLS 2011 public interop demo. The following sections describe the test cases executed and the results observed during the event. The majority of the tests needed more than the time allocated for the LEC event, but what was produced at the conclusion of a testing period is commendable.

1. MPLS Transport Profile

MPLS-TP technology facilitates the convergence of carriers' next generation networks onto a single transport technology. The MPLS-TP OAM is a subset of functions within the transport profile used for network performance monitoring, fault management and protection switching. It is a major building block within the MPLS-TP framework with capability to deliver carrier grade OA&M functions including sub-50ms traffic resiliency. In a nutshell, MPLS-TP enables MPLS to support packet transport services with a similar degree of predictability, reliability and OAM to those found in the existing transport networks.

Table 1 illustrates the point-to-point MPLS-TP (both single hop and multihop) LSPs that were created during the testing and indicates what vendor products participated in the testing. Comprehensive combinations of LSPs created confirm the stability and the readiness of the implementations, and adherence to the proposed standards.

Once the MPLS-TP LSPs were created, a few of the successful setups were chosen to verify the following tests:

a. CC/CV/RDI based on BFD
b. LSP Protection by BFD-based OAM
c. LSP Ping

The MPLS-TP OAM test bed comprised of network equipment from Cisco, NEC, Ixia and Spirent.

LER	LSR	LER
Cisco ASR9K		NEC CX2800
Cisco 7600		NEC CX2800
Cisco 7600		Ixia
Cisco ASR9K		Spirent
NEC CX2800		Spirent
NEC CX2800		Ixia
Cisco ASR9K	NEC	Cisco 7600
Cisco ASR9K	NEC	Spirent
NEC	7600	Ixia
Cisco ASR9K	NEC	Ixia

Table 1: Combinations of MPLS-TP LSPs tested

The LEC testing on MPLS-TP OAM started from the fundamental OAM based on BFD for a single LSP between two different vendor equipments. This test assumes the latest IETF draft, draft-ietf-mpls-tp-cc-cv-rdi. BFD sessions run in the coordinated mode. Devices were configured to initiate the BFD session setup by slow-start using the Poll-Final discipline.

Once the LSPs were set up with matching labels, BFD CC (Continuity Check) was enabled to monitor the continuity of the LSPs. BFD CC provides a rapid detection mechanism for LSP LOC (Loss of Continuity), in particular when lower layer may not be able to detect LOC failure at the LSP layer.

Many of the LSPs created were verified for pseudowire traffic. Similarly, LSP protection cases were verified with traffic. The failure triggers were initiated through fiber pull during the testing. LSP Ping using ACH (Associated Channel Header) was tested on each end of an LSP. Each LER supporting the functionality initiated LSP ping to the peering LER, in either a back-to-back configuration or through an LSP in the path, depending on the setup under test.

For LSP protection by BFD-based OAM, 1:1 path protection was tested between two different vendors and switching over from single-hop LSP to a multi-hop protected LSP and vice versa.

In the above tests, BFD CC sessions were running concurrently on both primary and backup LSP. When a BFD CC failure was introduced into the primary path, traffic successfully switched to the backup path. In addition, after the BFD CC failure was repaired, the

traffic successfully reverted back from the backup LSP to the primary LSP.

To demonstrate the use of two OAM toolsets of MPLS-based OAM and Y.1731 based OAM from ITU-T, multi-segment PW setup was planned traversing across two distinct OAM domains. In this area, we verified the interworking of multi-segment PW established by two distinct network domains, MPLS-based OAM domain and Y.1731-based OAM domain. In each domain, the MPLS-based OAM toolset including CC/CV, LSP-Ping, and the Y.1731-based OAM toolset including CCM, DM were operated, respectively.

For multi-segment PW, we attempted the user data through the statically provisioned multi-segment PW transport between a pair of CEs for the three cases listed below.

- Cisco ASR9000, NEC CX2800 and IXIA
- Spirent, NEC CX2800 and IXIA
- IXIA, NEC CX2800 and Spirent

In OAM testing, while the specific code-point for each MPLS-TP OAM function is still to be defined by IETF, we used the code-point values 0x7~0x9 for BFD and LSP Ping respectively, and the value within the experimental range for the Y.1731. We also verified the behavior of OAM functions within each domain.

Figure 3 shows the MPLS-TP setup that was used during the testing, in which Cisco, Ixia, Spirent and NEC participated.

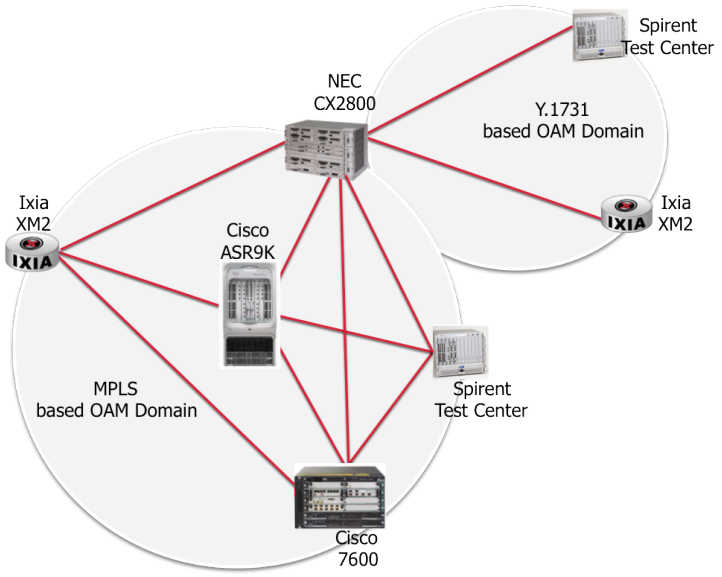

Figure 3: MPLS-TP Setup and Participants

2. BGP-mVPN using Point To Multipoint MPLS-TE

The scope of the testing was to demonstrate the forwarding of the customer multicast traffic across multiple vendor provider edge nodes using BGP-mVPN setup (refer figure 4). For the setup, the following scenarios were considered: PEs were placed in intra-AS setting using Inclusive Provider Multicast Service Interface (I-PMSI) with RSVP-TE as Provider tunnel. Sources were configured on the Juniper MX side, and receivers were configured on the Alcatel-Lucent 7750-SR side. Intra-AS mVPN membership discovery was performed via BGP mcast-vpn address family. Emulated CEs on the tester acting as the receiver were configured for IGMPv2 to receive the traffic from the source. The control plane verification tasks included the mVPN discovery, distribution of P-tunnel information and exchange of C-multicast routes. For the testing, we considered the following IETF proposed drafts:

a. draft-ietf-l3vpn-2547bis-mcast
b. draft-ietf-l3vpn-2547bis-mcast-bgp
c. draft-ietf-l3vpn-mvpn-considerations

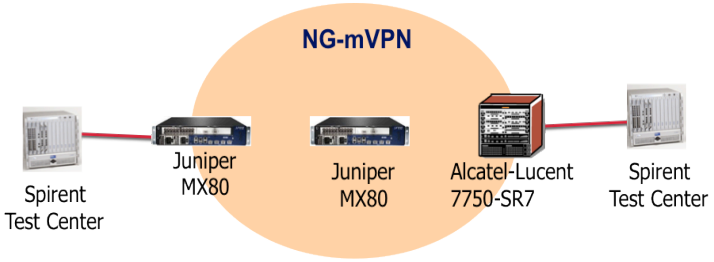

Figure 4: NG-mVPN setup considered

During the testing both Juniper MX80 and Alcatel-Lucent 7750-SR7 were configured as PE routers for Multicast VPN capability, with emulated receivers of multicast traffic (on the receiver PE side) and source simulated at the remote end (on the sender PE side). RSVP-TE LSPs was established between both the PEs and Inclusive PMSI (I-PMSI) tunnel type was used. The functionality was verified by Spirent Test Center that pushed the customer multicast traffic and validated the receiving of the same on the receiver PE side. Only Juniper Networks and Alcatel-Lucent participated in this part of the test.

3. MPLS Services over 100G Interfaces

For this test Ixia and Brocade offered 100 Gigabit Ethernet interfaces for interoperability participation. Brocade used their 100 G interface on the MLX-e

platform to connect with Ixia, which used the XM2 chassis to support 100 G forwarding and control plane. Figure 5 shows the topology considered for the 100 G tests.

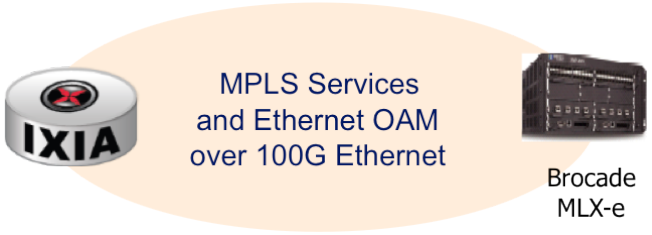

Figure 5: MPLS services over 100 G Link

The test was configured to demonstrate that services can be enabled and traffic can be comfortably forwarded for LDP based VPLS services and basic Ethernet connectivity fault management (CFM) defined in the IEEE 802.1ag can be supported on 100G interfaces. Ixia emulated the control plane functionality while performing the traffic generator role. Since only two vendors supported 100 G in the test, only 1-hop testing could be performed.

4. Ethernet Ring Protection Switching (ERPS) – G.8032

During the Fall LEC event, two vendors participated in the G.8032 interoperability. A simple two-node ring topology shown in Figure 6 was created to perform basic verification of the G.8032 functionality and various failure scenarios were created and behavior was observed. Ethernet Ring Protection protocol is defined in ITU-T G.8032 specifications, which integrates Automatic Protection Switching (APS) protocol and protection switching mechanisms to provide layer 2 loop avoidance and faster convergence in layer 2 ring topologies. ERP supports multi-ring and ladder topologies, however in this test a simple main ring topology was tested. ERP can also function with IEEE 802.1ag to support link monitoring when non-participating devices exist in the ring. Two participating devices were configured as Ring Protection Link (RPL) owner, non-RPL node and RPL node. At any time, the device can perform only one role.

The testing involved validation of Ring-APS messages between the two vendors at initial start-up and periodically when link or node failures or recoveries occur. The Ethernet Ring nodes forward the messages, if both the ports are in forwarding state and sending ERN terminates the message when it receives a message originally sent from it. During the testing ERP states were verified from Init to protection state, Manual-switch (MS), Forced-switch (FS) and pending. During the testing, various timers were verified to ensure the stability in the ring while a recovery is in progress or to prevent frequent triggering of the protection switching. We used the forced switch, which is an operator-initiated mechanism that moves the blocking role of the RL to a different link followed by unblocking the RPL.

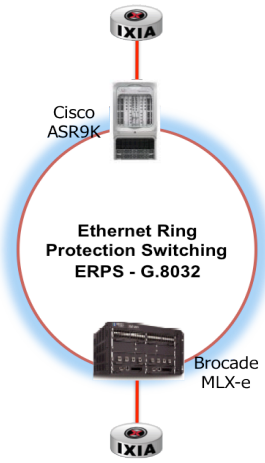

Figure 6: G.8032 Setup

Traffic forwarding validated all the states and the tester confirmed the recovery when failures were triggered. Figure 6 shows the topology that was considered for this test. Cisco and Brocade participated in this test.

5. Participating Products and Vendors

Alcatel·Lucent	7750-SR, 7710
CISCO	ASR 9000, CRS1, GSR XR12410, 7606
BROCADE	MLX-e
IXIA	XM2, IxNetwork
JUNIPER NETWORKS	MX80
NEC	CX2800
SPIRENT	TestCenter