



LINE CURRENT DIFFERENTIAL PROTECTION OVER MPLS

*Juniper, SEL provide end-to-end packet-switched
communications for control and protection*

TABLE OF CONTENTS

Introduction	3
Line Current Differential Protection	4
Supporting Line Current Differential Protection over MPLS	4
Latency.....	4
Asymmetry	4
Channel Restoration Time	4
Proof of Concept Test Bed.....	6
Establishing Logical Ring	6
Performance Test Results	7
1. SEL Inc. ICON-to-ICON Base Measurement—Direct Fiber (No MPLS Network)	7
2. ICON-to-ICON Base Measurement—Juniper MPLS Network.....	7
3. Primary Path Interruption at the SEL ICON	7
4. Primary Path Restoration at the SEL ICON	8
5. Primary Path Interruption in the Access Layer of the Juniper MPLS Network	8
6. Primary Path Restoration in the Access Layer of the Juniper MPLS Network	8
7. Primary Path Interruption in the Core Layer of the Juniper MPLS Network.....	9
8. Primary Path Restoration in the Core Layer of the Juniper MPLS Network	9
9. Primary Path Traffic Interruption in the Core Layer of the Juniper MPLS Network Without Circuit Failure	9
10. Primary Path Traffic Restoration in the Core Layer of the Juniper MPLS Network Without Circuit Failure	10
Overall Results	10
Conclusion	10
About Juniper Networks	11

EXECUTIVE SUMMARY

Juniper Networks, a global leader in networking and cybersecurity, and SEL Inc., a global leader in control, protection, and communications infrastructure for the electrical grids, have joined forces to develop a simplified, SDN-automated solution for IT-OT convergence. The Juniper-SEL Converged Industrial Edge for Utilities solution bridges the gap between legacy synchronous services and new packet-switched architectures; meaning that, in addition to OT-SDN and IEC61850 Ethernet for substation modernization, a full range of legacy serial and time-division multiplexing (TDM) circuit types can safely traverse packet-switched WANs with their latency, asymmetry, and network healing attributes intact.

The Juniper-SEL Inc. solution is designed to support all grid applications, from low-speed, high-latency supervisory control and data acquisition (SCADA) to deterministic, low-latency teleprotection, which requires millisecond fault identification, transmission, notification, and resolution. For the purposes of this paper, the Line Current Differential teleprotection application was used to test the solution architecture and produce the performance test results, which demonstrate the effectiveness of SEL Inc.'s Virtual Synchronous Networking (VSN) Ethernet encapsulation of synchronous protocols supporting Line Current Differential Protection over Juniper's MPLS WAN technologies. Overall, the testing confirms packet-switched architectures can perform critical control and protection applications without impact to the safety and reliability of the grid, while providing new architectural flexibility for longer term modernization programs.

Appropriate for both greenfield and brownfield deployments, Juniper and SEL Inc. offer an open, standards-based solution designed to modernize the centralization of control, management, policy, and orchestration, increasing situational awareness and reducing complexity and OpEx.

Introduction

Historically, the communications underlying the control of grid protection equipment has relied on SONET/SDH and other forms of synchronous, time-division multiplexing technologies. The deterministic nature of TDM was well suited to the latency, symmetry, and jitter requirements of critical utility control and protection applications. SONET and TDM were rightly seen as low risk and were widely deployed in the Public Switched Telephone Network (PSTN). Their pedigree was unquestioned.

Like the older PSTN, however, the requirements of grid communications have changed significantly. The introduction of paradigm-challenging developments at the grid edge have utilities evaluating their next generation of communication networks with scale, management visibility, and automation in mind. Applications like Automated Metering Infrastructure (AMI), Demand Response (DR), and Distributed Automation (DA) reduce OpEx and create potential new revenue streams for utilities, but they almost exclusively use packet-switched communications technologies in the WAN, substation, and Field Area Network (FAN) to provide the needed scale, visibility, and resiliency. Grid modernization enables a diverse set of applications, but the brownfield nature of most utility field communications systems means legacy TDM and serial communications must be integrated with packet-switched communications systems or risk becoming isolated and stranded. This requires separate support staffing and maintenance contracts, which increases operations cost and risk.

This is the paradox that must be resolved. How do utilities adopt modern packet-switched technologies to support new applications while maintaining the deterministic communications requirements of legacy serial and TDM-based control and protection equipment? This paper will describe the performance of the Juniper-SEL Converged Industrial Edge for Utilities solution within the context of a stringent use case: providing protection communications for Line Current Differential Protection using packet-switched backhaul without requiring upgrades to the existing grid protection infrastructure.

Line Current Differential Protection

The line current differential protection principle is widely used across modern power systems because of its immunity to changing system conditions, ability to detect nontraditional sources of fault currents, excellent sensitivity, good performance on multiterminal and series-compensated lines, and simplicity of application from the point of view of traditionally understood protection engineering practices.

Communications channels traditionally used for line current differential protection are limited in bandwidth (64 kbps is common) and based around a synchronous serial scheme. Interface standards such as IEEE C37.94 and G.703 are commonly used. The performance characteristics of the communications channel and timing alignment method are critical to both the security and dependability of line current differential protection schemes. Individual circuits are easily groomed into higher level digital hierarchy formats (like T1, E1, or STS-1) and transmitted over synchronous wide area networks. This communications scheme represents the status quo for applications like Line Current Differential today.

Supporting Line Current Differential Protection over MPLS

Improvements to operating cost, management visibility, scalability, and feature velocity are just a few of the reasons why utilities are considering migration to packet-switched wide area communications networks, like MPLS. To meet stringent operations technologies (OT) requirements and ensure reliability, the challenge of engineering line current differential protection circuits over a packet network must be addressed—specifically as it pertains to network healing requirements and communications channel restoration times.

Latency

The speed at which the protection scheme operates is dependent on the combination of internal relay data latencies, algorithm processing time, and communications channel delay. The faster a fault can be detected, the faster the breaker can be tripped, reducing the amount of time faulty current is flowing. This reduces wear on critical transmission components, enables faster power restoration, and, in many cases, saves lives. For critical transmission lines, IEC 61850-90-12 specifies a 5 ms or less latency requirement for line current differential communication circuits.

Asymmetry

Line current differential schemes that use channel-based timing can't operate with a channel asymmetry worse than one quarter power cycle (4 ms), and some relays have even less tolerance. To achieve data alignment accuracy of 1 electrical degree requires channel asymmetry of 0.05 ms or better. For high sensitivity, high-speed line current differential schemes, 0.5 ms channel asymmetry is required.

Channel Restoration Time

Line current differential protection implementations are very sensitive to data loss. Some relays will interpolate data from a single missing data packet, but to prevent risk of a mis-operation, the loss of successive data packets will force the relay to block the differential protection element until the communications channel is restored and a confidence window of data has been received. Depending on how long the communications channel is lost, the relays may need to completely resynchronize, which blocks the differential element for a much longer period. Achieving a restoration time of 5 ms or less guarantees minimal impact to the line current differential protection function, ensuring the highest level of protection to critical power transmission systems.

To date, packet transport technologies such as MPLS have had difficulty meeting the stringent communication channel requirements for line current differential. They were unable to offer the same guaranteed latency, asymmetry, and failover performance as protection-class SONET systems due to their asynchronous shared bandwidth approach, which is optimized for efficiency and delivering multiple services with varying traffic loads. The Juniper-SEL Converged Industrial Edge for Utilities solution proves this perception is no longer valid. By combining the advanced Virtual Synchronous Networking (VSN) feature set of the SEL Integrated Communications Optical Network (ICON) multiplexer with Juniper's fine-grained, best-of-breed class of service (CoS), utilities can now safely operate sophisticated protection schemes like line current differential and direct transfer trip, while reaping the cost, scale, and control benefits of MPLS. SEL Inc.'s VSN modules for the ICON platform replace SONET primary and backup line modules with Ethernet line modules. All other ICON modules are preserved, so utilities can continue using existing protection equipment and protection schemes.

SEL Inc.'s VSN provides a way to transport serial teleprotection channels (such as IEEE C37.94) over MPLS while maintaining synchronous performance. This technology allows utilities to preserve communication channel performance for their protection applications after migrating from a T1 or SONET system to one using MPLS.

VSN technology works by maintaining a synchronous network and preserving a SONET engine function. The SONET subsystem provides a synchronous interface for each teleprotection serial circuit. The SONET subsystem is then encapsulated in an Ethernet transport system, packetizing the native SONET data at the VT1.5 or synchronous transport signal (STS) level (rather than DS0) to be more bandwidth-efficient. The Ethernet packets are standard Layer 2 frames that contain the SONET data along with synchronization information and the network management system (NMS) channel.

To maintain the synchronous operation of the SONET engine, Ethernet packets are transmitted at regular intervals. The Juniper MPLS network is configured to ensure acceptable packet-delay tolerance, allowing the system to maintain synchronous operation. The VSN implementation is shown in Fig. 1. The network requires much smaller jitter buffer sizes to manage the packet delay variation (PDV) through the core network. Typical jitter buffer sizes are in the 100-150 us range, vs. 3-5 ms for pseudowire approaches.

By maintaining the synchronous principle of SONET, VSN technology can transport serial circuits with almost the same performance as a native SONET network.

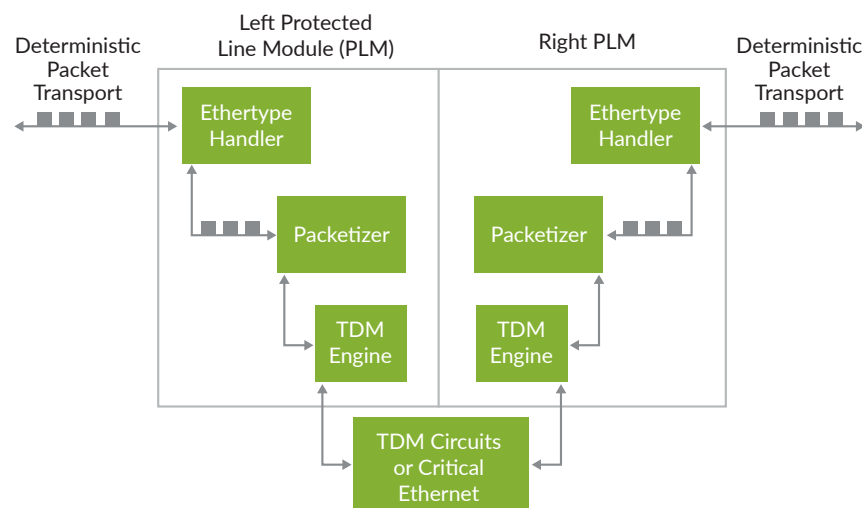


Figure 1: Virtual Synchronous Networking (VSN) implementation

Proof of Concept Test Bed

Juniper and SEL Inc. established a Converged Ethernet Grid solution Proof of Concept Lab (POL Lab) in April of 2018. Engineers from both companies set up and tested the Juniper-SEL Converged Industrial Edge for Utilities solution against a set of communications node models, representing grid communications requirements for distribution and transmission substations and nonelectrical transit, aggregation, and core sites. Circuit-switched communication channel requirements were tested using T1 uplink ports, FXS ports, T1 ports, 4 wire ports, C37.94 ports, RS232 ports, and Ethernet ports. The communications node models were designed to represent the current state of, and future requirements for, reliable communications capabilities supporting the utility market for the next era of digitalization and packetization.

The proof of concept lab utilizes Juniper Networks® MX Series 5G Universal Routing Platforms configured as an MPLS logical mesh network with “north” and “south” paths. Representing the access and core layers of the network, the MX Series routers were interconnected using 1GbE and 10GbE, respectively. The MX Series routers connected to the SEL ICONs running VSN were configured as MPLS provider edge (PE) routers, while the intermediate MX Series core routers were configured as MPLS provider (P) routers. VSN traffic generated from the SEL ICON received the highest priority CoS, guaranteed bandwidth, and strict scheduling. All tests were performed under maximum load created by multiple packet generators.

Establishing Logical Ring

The SEL ICONs were configured to encapsulate and transport L2 Ethernet VSN traffic at multiple committed information rates ranging from 10 Mbps (6 x T1 encapsulated) to 120 Mbps (1 x STS-1). Control traffic from the SEL 411L Line Differential Protection relay was transmitted across both north and south paths. Fixed or static paths were provisioned across the core to create a ring topology. A ring topology has several benefits:

- It bundles all substation circuits into a single static path, which reduces the complexity associated with provisioning and managing separate paths for each protection circuit on the MPLS network.
- It creates a demarcation between IT and OT, allowing the protection circuits to be managed by the OT team.
- It allows failover to be performed by the VSN OT edge device, which enables very fast failover (less than 5 ms).

The MX Series routers were configured with label-switched paths (LSPs) forming the ICON paths. The ICON determined endpoint reachability and fast reroute for the ICON data streams. The following test results validate the performance of line current differential protection through a set of tests involving SEL 411L relays, SEL ICON multiplexers, and an MPLS network made up of MX Series routing platforms.

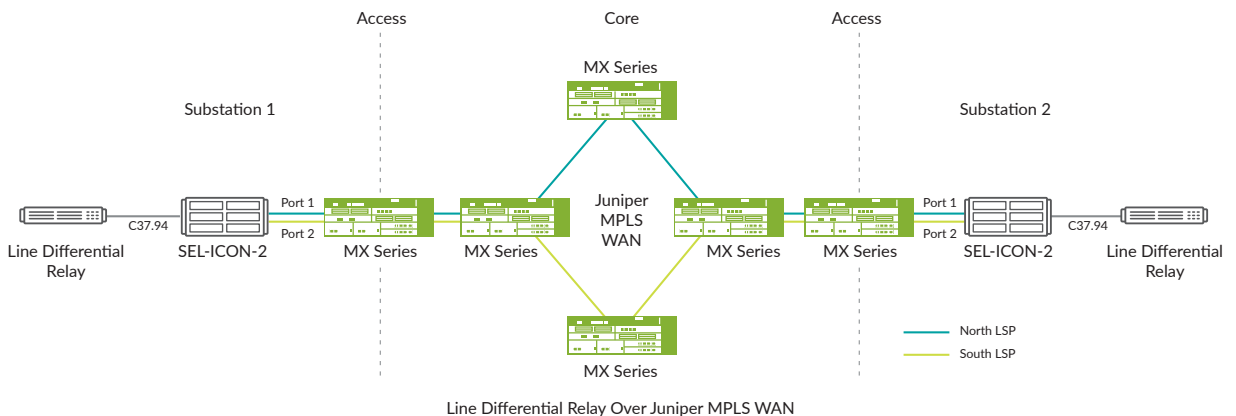


Figure 2: Juniper-SEL converged Ethernet test bed

Performance Test Results

The test scenarios and testing results are as follows:

1. SEL Inc. ICON-to-ICON Base Measurement—Direct Fiber (No MPLS Network)

Description: The SEL ICONs were connected in a collapsed ring configuration with a primary and backup path over direct fiber optic connections. End-to-end readings were taken from SEL 411L to SEL 411L over direct fiber.

Narrative: This test was conducted to establish a baseline reading of current differential relay from SEL 411L to SEL 411L prior to connection through the MPLS core network.

Table 1: Test 1 Results

STATISTICS	Channel 1	Channel 2
Round-Trip Delay (ms)	1.0	1.0
Transmit Delay (ms)	0.5	0.5
Receive Delay (ms)	0.5	0.5
Asymmetry (ms)	0.00	0.00
411L Lost Packet Count	0	0

2. ICON-to-ICON Base Measurement—Juniper MPLS Network

Description: The SEL ICONs were connected to, and through, the Juniper MPLS network.

Narrative: This test was conducted to establish a baseline reading of the SEL 411L current differential relay when connected through the Juniper MPLS network.

Table 2: Test 2 Results

STATISTICS	Channel 1	Channel 2
Round-Trip Delay (ms)	1.1	1.1
Transmit Delay (ms)	0.6	0.5
Receive Delay (ms)	0.5	0.6
Asymmetry (ms)	0.09	0.09
411L Lost Packet Count	0	0

Note: All subsequent tests were made with the Juniper MPLS network in place.

3. Primary Path Interruption at the SEL ICON

Description: The SEL ICON line protection module configured for the primary path transport of line ports across the Juniper MPLS core network was turned down via control software.

Narrative: This test was conducted to cause a switch from the primary path to the backup path and to measure the impact on the SEL 411L current differential relay.

Table 3: Test 3 Results

STATISTICS	Channel 1	Channel 2
Round-Trip Delay (ms)	0.9	0.9
Transmit Delay (ms)	0.5	0.4
Receive Delay (ms)	0.4	0.5
Asymmetry (ms)	0.12	0.12
411L Lost Packet Count	2	1

4. Primary Path Restoration at the SEL ICON

Description: The SEL ICON's primary path was restored by reinitializing the primary path line ports on the ICON-protected line module.

Narrative: This test was conducted to cause a reversion from the network backup path to the primary path; and to measure impact on the SEL 411L current differential relay protection.

Table 4. Test 4 Results

STATISTICS	Channel 1	Channel 2
Round-Trip Delay (ms)	0.9	0.9
Transmit Delay (ms)	0.5	0.4
Receive Delay (ms)	0.4	0.5
Asymmetry (ms)	0.12	0.12
411L Lost Packet Count	0	0

5. Primary Path Interruption in the Access Layer of the Juniper MPLS Network

Description: The primary path port on the Juniper MPLS access router was turned down via control software.

Narrative: This test was conducted to simulate a network failure at the access layer and to measure the impact to line current differential protection of a switch from the primary path to the backup path by the SEL ICON across the Juniper MPLS core network.

Table 5. Test 5 Results

STATISTICS	Channel 1	Channel 2
Round-Trip Delay (ms)	1.0	1.0
Transmit Delay (ms)	0.5	0.5
Receive Delay (ms)	0.5	0.5
Asymmetry (ms)	0.00	0.00
411L Lost Packet Count	1	2

6. Primary Path Restoration in the Access Layer of the Juniper MPLS Network

Description: The primary path port on the Juniper MPLS access router was reinitialized via control software.

Narrative: This test was conducted to simulate a network failure restoration at the access layer and to measure the impact to line current differential protection of a switch from the backup path to the primary path by the SEL ICON across the Juniper MPLS network.

Table 6. Test 6 Results

STATISTICS	Channel 1	Channel 2
Round-Trip Delay (ms)	1.1	1.1
Transmit Delay (ms)	0.6	0.5
Receive Delay (ms)	0.5	0.6
Asymmetry (ms)	0.12	0.12
411L Lost Packet Count	0	1

7. Primary Path Interruption in the Core Layer of the Juniper MPLS Network

Description: The primary path port on the Juniper MPLS CORE router was turned down via control software.

Narrative: This test was conducted to simulate a network failure in the MPLS network core and to measure the impact to line current differential protection of a switch from the primary path to the backup path by the SEL ICON across the Juniper MPLS network.

Table 7. Test 7 Results

STATISTICS	Channel 1	Channel 2
Round-Trip Delay (ms)	1.1	1.1
Transmit Delay (ms)	0.6	0.5
Receive Delay (ms)	0.5	0.6
Asymmetry (ms)	0.12	0.12
411L Lost Packet Count	1	3

8. Primary Path Restoration in the Core Layer of the Juniper MPLS Network

Description: The primary path port on the Juniper MPLS core router was reinitialized via control software.

Narrative: This test was conducted to simulate a network failure restoration in the MPLS network core and to measure the impact to line current differential protection of a switch from the backup path to the primary path by the SEL ICON across the Juniper MPLS core network.

Table 8. Test 8 Results

STATISTICS	Channel 1	Channel 2
Round-Trip Delay (ms)	1.1	1.1
Transmit Delay (ms)	0.6	0.5
Receive Delay (ms)	0.5	0.6
Asymmetry (ms)	0.11	0.11
411L Lost Packet Count	0	0

9. Primary Path Traffic Interruption in the Core Layer of the Juniper MPLS Network Without Circuit Failure

Description: The control traffic on the primary path of the Juniper MPLS network was redirected to a NULL interface, leaving the primary path circuit up and running.

Narrative: This test was conducted to illustrate the SEL ICON's ability to detect loss of traffic without the loss of a physical or logical circuit and to measure the impact to line current differential protection of a switch to the backup path. This test illustrates the resilience of the Juniper-SEL solution in the case of MPLS core misconfiguration that results in traffic being inadvertently "blackholed."

Table 9. Test 9 Results

STATISTICS	Channel 1	Channel 2
Round-Trip Delay (ms)	1.0	1.0
Transmit Delay (ms)	0.5	0.5
Receive Delay (ms)	0.5	0.5
Asymmetry (ms)	0.00	0.00
411L Lost Packet Count	2	2

10. Primary Path Traffic Restoration in the Core Layer of the Juniper MPLS Network Without Circuit Failure

Description: The control traffic on the primary path of the Juniper MPLS network was restored from the NULL interface, resulting in a switch back to the primary path from the backup path.

Narrative: This test was conducted to illustrate the SEL ICON's ability to detect restoration of control traffic from the misconfiguration and to measure the impact to line current differential protection of a switch to the primary path.

Table 10. Test 10 Results

STATISTICS	Channel 1	Channel 2
Round-Trip Delay (ms)	1.0	1.0
Transmit Delay (ms)	0.5	0.5
Receive Delay (ms)	0.5	0.5
Asymmetry (ms)	0.00	0.00
411L Lost Packet Count	2	2

Overall Results

A slight increase in latency (approximately 100 microseconds) occurred when connecting through the core network with no impact to asymmetry and switch times. Performance was maintained using the SEL ICON to manage protective relaying circuits.

Conclusion

Utilities' natural inclination toward risk avoidance has colored their view of information technologies and IT industry delivery practices. Generally, this has caused a lag in adoption of IT for Operations environments.

However, a confluence of trends has merged to catalyze the initiation, operationalization, and scaling of modernization projects. Budgetary pressure to find operational efficiencies that reduce costs has mounted. Packet-switched and software-defined network (SDN) technologies, created to address the security, performance, and automation/scaling problems of the largest and most mission-critical networks, have entered the mainstream with a proven track record of reducing complexity, abstracting technical layering, and delivering elevated levels of service and capabilities for critical applications. Meeting or exceeding most stringent OT requirements for current differential protection and other real-time traffic is empirically proven, and these technologies continue to gain in feature velocity and maturity for their operational models—all while cost per bit is falling year over year.

Juniper Networks and SEL Inc. are embracing these trends to provide our customers with solutions for the new generation of digitalization. It's best-of-breed engineering—simplified.

About Juniper Networks

At Juniper Networks, we are dedicated to dramatically simplifying network operations and driving superior experiences for end users. Our solutions deliver industry-leading insight, automation, security and AI to drive real business results. We believe that powering connections will bring us closer together while empowering us all to solve the world's greatest challenges of well-being, sustainability and equality.

About SEL Inc.

SEL specializes in creating digital products and systems that protect, control, and automate power systems around the world. This technology prevents blackouts and improves power system reliability and safety at a reduced cost. A 100 percent employee-owned company headquartered in Pullman, Washington, SEL has manufactured products in the United States since 1984 and serves customers worldwide. As part of our commitment to designing and manufacturing reliable, HYPERLINK "<https://selinc.com/company/quality-philosophy/>"high-quality products, we research, design, build, test, distribute, teach, and support each of our technologies at SEL facilities. Assembled SEL products travel directly from our hands to where they need to be, so we feel confident that you and your customers can rely on them to keep critical systems fully operational.

Corporate and Sales Headquarters

Juniper Networks, Inc.
1133 Innovation Way
Sunnyvale, CA 94089 USA
Phone: 888.JUNIPER (888.586.4737)
or +1.408.745.2000
Fax: +1.408.745.2100
www.juniper.net

APAC and EMEA Headquarters

Juniper Networks International B.V.
Boeing Avenue 240
1119 PZ Schiphol-Rijk
Amsterdam, The Netherlands
Phone: +31.207.125.700



Copyright 2021 Juniper Networks, Inc. All rights reserved. Juniper Networks, the Juniper Networks logo, Juniper, and Junos are registered trademarks of Juniper Networks, Inc. in the United States and other countries. All other trademarks, service marks, registered marks, or registered service marks are the property of their respective owners. Juniper Networks assumes no responsibility for any inaccuracies in this document. Juniper Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice.