Alcatel-Lucent
1850 Transport Service Switch®
MPLS-TP Packet Transport Protection Performance

Introduction

Alcatel-Lucent commissioned the European Advanced Networking Test Center (EANTC) to verify the performance of their packet transport protection mechanisms as implemented in the 1850 Transport Service Switch (TSS). The tests were conducted at EANTC's lab in Berlin in January 2010. EANTC engineers evaluated the devices according to a detailed test plan.

According to Alcatel-Lucent the Devices Under Test (DUTs), targeted at the service provider market, are designed as "packet-optical transport platform to build scalable and reliable packet transport networks and support Carrier Ethernet services". With such a mission statement the 1850 TSS-series must fulfil service provider fundamental requirements from their transport solutions: scalability, robustness and resiliency.

Alcatel-Lucent 1850 TSS®

☑ Failure Recovery
Deterministic performance

☑ Service Protection
Reliable and scalable

Test Period: January 2010
1850 TSS-320 and TSS-160
Release 3.20
© 2010 EANTC AG

Tested by EANTC 2010

Test Highlights

- ➜ **Support for up to 4,000 fully protected MPLS-TP tunnels**
- ➜ **Maximum failure recovery as low as 34.2 ms**
- ➜ **As low as 12.7 ms out of service time for 1,332 MPLS-TP tunnels**

Tested Devices & Test Equipment

Alcatel-Lucent provided the 1850 TSS-320 as well as its compact chassis version, the 1850 TSS-160, for the testing. Both Network to Network (NNI) and User to Network (UNI) interfaces were configured using Ethernet blades. MPLS Transport Profile (MPLS-TP) was used between the DUTs themselves while plain Ethernet was used on the UNI ports which were connected to the Spirent TestCenter traffic generator.

Alcatel-Lucent offered the following description of the product: The 1850 Transport Service Switch (TSS) is a next generation Packet Optical Transport platform for mobile and fixed broadband aggregation from access to metro-core. The platform supports reliable aggregation of any traffic mix from circuits to packets with deterministic performance and hardware-implemented OAM tools.

The Alcatel-Lucent 1850 TSS-320

Test Goal

The success of a packet transport network depends on two main aspects: Its ability to service a growing number of customers and its adherence to Service Level Agreements (SLAs) with said customers. One aspect of guaranteeing high SLAs to customers is the ability to maintain network services in the face of failure. Automatic failure recovery, at scale, is a benchmark set by legacy transport networks, and must be implemented in packet transport networks especially given the nature of data carried over these networks: voice, video, financial transactions and business critical data.

The testing goal was to show that the MPLS-TP packet transport solution provided by the Alcatel-Lucent 1850 TSS can offer service providers the peace of mind they require with respect to service continuity. Alcatel-Lucent asked us to verify that their solution can deliver the service recovery benchmark set in the networking industry - 50 milliseconds. Not only were we to verify that upon failure in the network the services could continue operating, but also, we verified that this protection performance applied to the maximum number of protected tunnels supported on the system.

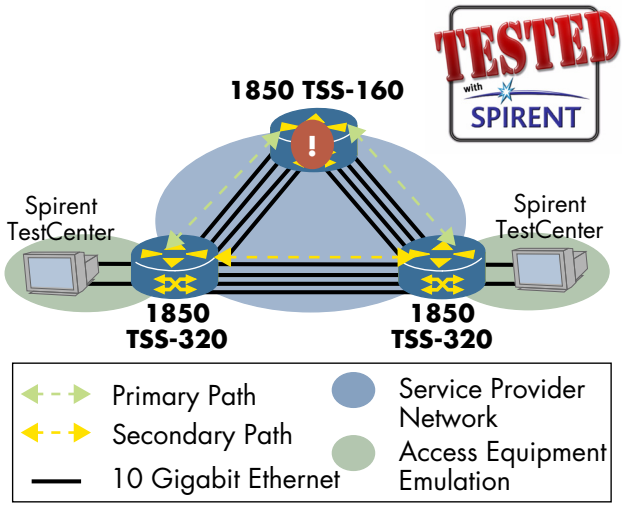

Figure 1: Test Setup

Test Setup

Alcatel-Lucent engineers set up a test topology in our lab consisting of two 1850 TSS-320s and one 1850 TSS-160 (as depicted in the figure above). Two physical paths were configured in the network - one working, through the 1850 TSS-160 and the second, recovery, directly between the two 1850 TSS-320.

This configuration allowed us to shut down all links in the working path between the devices, emulating a sudden conduit failure that will severe all services transported over those links.

As Alcatel-Lucent states, the 1850 TSS platform implements in hardware its MPLS-TP based Operations Administration and Maintenance (OAM) mechanisms - the essential tools for immediate failure detection. The devices support different Continuity Check Message (CCM) transmission periods (intervals) for OAM running over tunnels (Label Switched Paths - LSPs). Two such intervals were used for our testing. One set of tests was performed with CCM intervals of 10 milliseconds (ms) and a second set used the more aggressive 3.3 ms interval. As is generally the rule, nothing in life comes for nothing. When using 3.3 ms CCM interval the devices could protect up to 1,332 tunnels. The maximum number of protected tunnels (4,000) could be reached when using 10 ms CCM interval.

Our test used Ethernet services to emulate customers being transported across the test network. Each Ethernet service was mapped to a single protected tunnel resulting in 4,000 tunnels (VLAN mapped) for the test which used 10 ms CCM interval, and 1,332 tunnels for the test using 3.3 ms CCM interval.

Test Execution

We conducted individual test runs for each CCM interval. We started each test by generating traffic and then abruptly disconnecting the power from the 1850 TSS-160 device. This phase of the test was called protection. After we had analyzed the results for the protection test we started sending traffic again and then reconnected the failed device to its power. This phase of the test was called restoration. In order to verify that the results were consistent we repeated the sequence (protection followed by restoration) at least three times.

We used Spirent's TestCenter with software version 3.30 for the testing alongside Spirent's HyperMatrix 10 GbE interfaces. The tester emulated customer traffic and measured the out of service time caused by the failover we emulated in the test network.

Test Results

Both test sets (for the two CCM intervals) produced remarkably consistent results. The highest out of service time we recorded during the protection phase of the 10 ms CCM interval test was 36.5 ms with consecutive test runs producing only slight variations: 35.6 ms and 34.2 ms. Along the same lines the protection phase of the 3.3 ms CCM interval tests produced at most an out of service time of 14 ms and in the other two test runs 12.7 and 13.7 ms service interruption.

As is seen in the graphs on this and the following page, the restoration phase of the testing produced consistent results as well. All backup paths were configured in revertive mode such that as soon as the working path returned to operations the working path would be used. The devices implement the wait to restore (WTR) timer and waited 60 seconds from the time the working path was established before switching traffic to it. This mechanism, as per best practice in transport networking, attempts to protect the system from instability which would be caused if the working path is still experiencing issues and traffic has been switched to it.

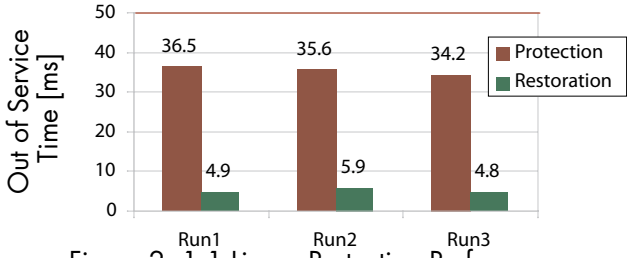

Figure 2: 1:1 Linear Protection Performance Verification - 10 ms CCM Interval

We were also able to precisely characterize the service interruption behavior using the Spirent TestCenter. We configured a trigger which allowed us to

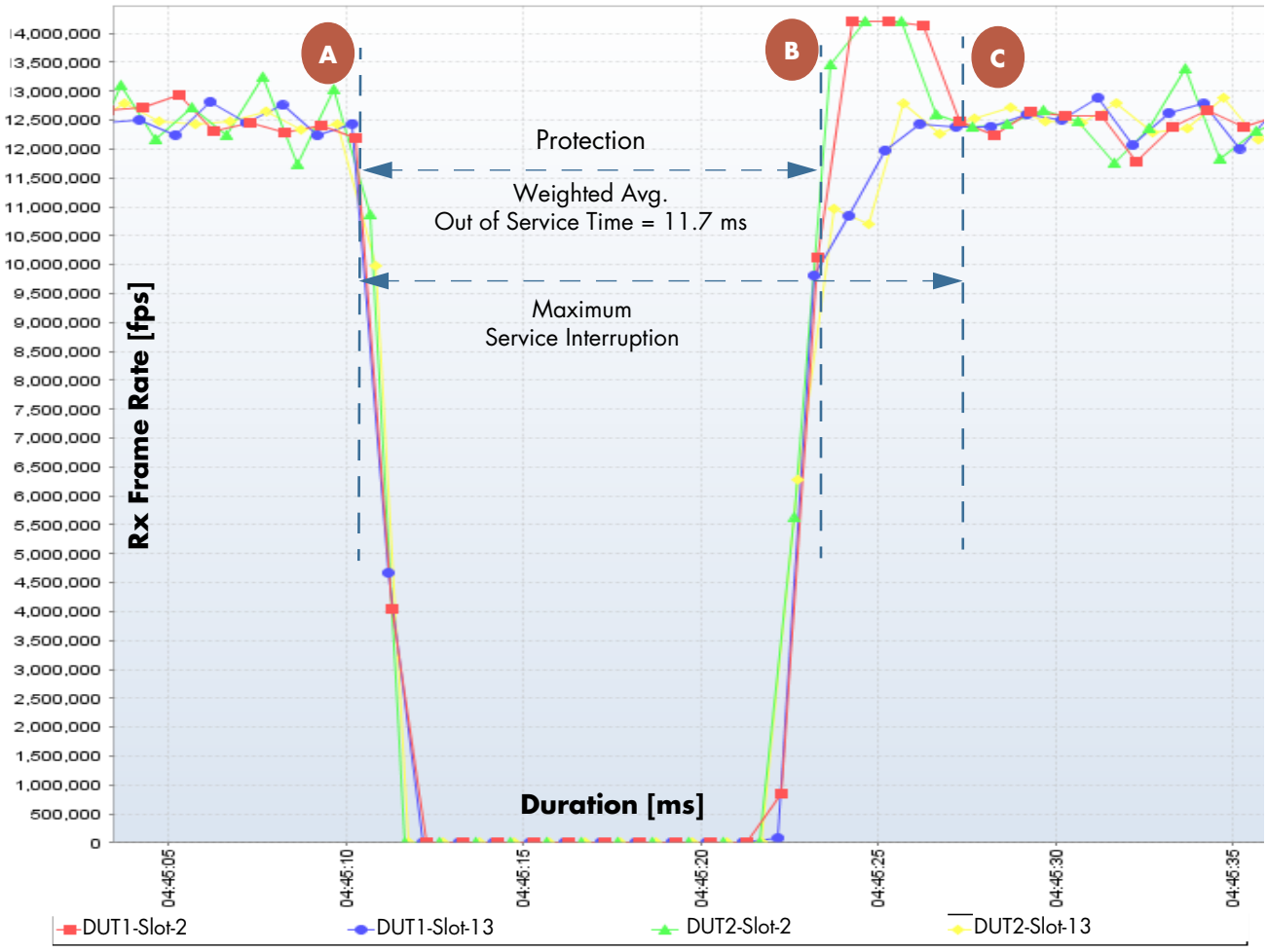

Figure 3: Service Interruption During 10 ms CCM Interval Test (Example)

sample, at 1 ms intervals, the reception of test frames on all ports in the test. Using this methodology we produced Figure 3 that actually shows the service interruption during one of the simulated failure conditions. Point A marks the instance at which we failed the 1850-160 TSS, point B depicts the first port to completely return to operations and point C shows all ports in a stable and normal operations.

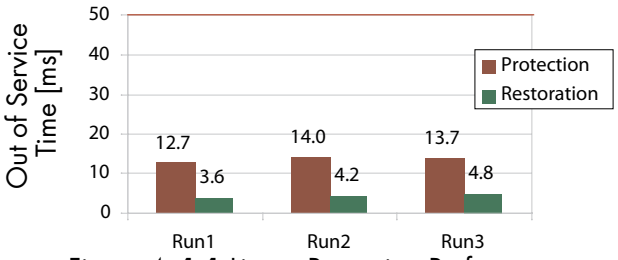

Figure 4: 1:1 Linear Protection Performance Verification - 3.3 ms CCM Interval

We also noted the proportional relationship between the configured CCM intervals in each of the tests and the results. The 3.3 ms CCM interval tests produced an out of service time roughly one third of that recorded in the 10 ms CCM interval test. This was the expected theoretical behavior and we were pleased to see that the theory met the observation.

Figure 5: The Test Bed Setup at EANTC

Summary

The results recorded in the test demonstrated that the protection switching performances of the 1850 TSS-320 were reliable, consistent and reproducible - elements essential to the operations of modern networks. The results were, in all test runs, well below the industry benchmark of 50 ms. With packet networks being the backbone of the 21st century economy such predictability, dependability, and deterministic performance to ensure business continuity is essential.

We showed that the solution was able to protect all tunnels at scale. Using 10 ms CCM interval all 4,000 were protected. With the more aggressive failure detection of 3.3 ms CCM interval, the device showed a reduction in the number of MPLS-TP tunnels that could be protected while delivering faster protection performance. Service providers that require such aggressive failure detection should be ready to make the compromise between the number of protected tunnels and the high service availability. All in all the solution's protection performance delivered on the target set by Alcatel-Lucent for their system and is well in line with service providers' requirements for scalability, availability and deterministic performance of packet transport networks.

About EANTC

The European Advanced Networking Test Center (EANTC) offers vendor-neutral network test services for manufacturers, service providers and enterprise customers. Primary business areas include interoperability, conformance and performance testing for IP, MPLS, Mobile Backhaul, VoIP, Carrier Ethernet, Triple Play, and IP applications.

EANTC AG
Einsteinufer 17, 10587 Berlin, Germany
info@eantc.com, http://www.eantc.com/

JG, V1.3, 20100204