

Rohde & Schwarz R&S® SITLine ETH Crypto Device Performance & Interoperability Tests

Introduction

Rohde & Schwarz SIT commissioned the European Advanced Networking Test Center (EANTC) to verify the performance and interoperability of the new R&S SITLine ETH Crypto Device. The tests were conducted at the EANTC test lab in Berlin in January and April 2008. EANTC test engineers conducted the tests according to a detailed test plan written by EANTC to verify interoperability and performance of the new Rohde & Schwarz Crypto device.

EANTC tested the Ethernet performance, support of the Metro Ethernet Forum (MEF) E-Line service type and the interoperability with Cisco Catalyst series switch. The results confirmed the capability of the crypto device to encrypt Ethernet traffic with imperceptible repercussion on network performance. The SITLine ETH does add neither excessive latency nor significant security overhead.

Test Highlights

- Interoperability with Cisco Catalyst
- Support of Carrier Ethernet MEF E-Line service type
- Negligible latency by encryption device
- Transparent transport of IEEE CFM and EFM OAM frames based on hardware filter
- Line rate throughput
- Long term service stability

Tested Devices & Test Equipment

The R&S SITLine ETH encrypts Ethernet Frames. Two variants of the device were tested:

- 2-port (1 line) Gigabit Ethernet device: SITLine ETH1G
- 8-port (4 line) Fast Ethernet device: SITLine ETH100

The SITLine ETH has been designed so that each public port is logically connected to one private port. One public and one private port form together one line. The two port device supports one Gigabit Ethernet line and the eight port device supports four 10/100 Ethernet lines. On the private ports the plain Ethernet traffic comes in and out towards the customer. On the assigned public ports the data leaves the device encrypted or is received for decryption.



Rohde & Schwarz SIT R&S® SITLine ETH

- X** Ethernet Performance
Line rate throughput
- X** MEF E-Line Support
IEEE CFM & EFM OAM transport
- X** Service Stability
Over long term usage

Test Period: January and April 2008
© 2008 EANTC AG
<http://www.eantc.com>



The devices support two modes:

- Tunnel mode: The received Ethernet frames will be encrypted in their entirety and tunneled using an additional Ethernet frame plus a 4 Byte security encryption header.
- Transport mode: No additional overhead, only the payload is encrypted.

The additional overhead for the crypto function in both modes is extremely low – only one 64 Byte Ethernet Frame is transmitted every 60 seconds to check whether both devices still use the common secure key (secure link check). Six Ethernet Frames are exchanged after a selectable interval to update the secure key (session key update).

The testing environment included a Spirent Smartbits 6000B tester, Cisco Catalyst 6509, Cisco Catalyst 7206 and two Riverstone RS8000 routers. The Cisco devices were used in the raw mode Pseudowire test as seen in the figure below while the Riverstones were used in the tagged mode Pseudowire test.

Functionality & Interoperability

The goal of these tests was to verify the functionality of the encryption solution and the interoperability with popular switch components.

Test Highlights

- MPLS pseudowire raw mode
- MPLS pseudowire tagged mode
- Perfect handling of bursty traffic
- Hardware filters performance

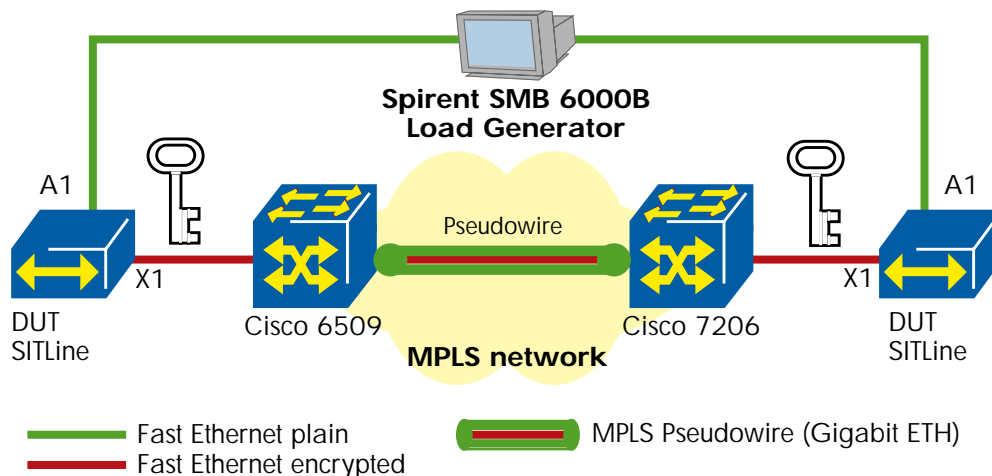
MPLS Pseudowire – RAW Mode

Numerous Ethernet Private Line (EPL) services are implemented in the field using MPLS Pseudowires which is why we tested the SITLine ETH ability to be used over MPLS pseudowires. Other solutions such as Provider Backbone Bridges (PBB) and T-MPLS are also available, but were not tested here. We see no technical reason why the SITLine should not work properly on MEF conformant Ethernet connections over PBB or T-MPLS.

We verified that the Rohde & Schwarz SITLine ETH encryption device was able to encrypt Ethernet traffic to be transported over MPLS Pseudowire connections. The challenge for the encryption device was to add additional headers to the user traffic and then to communicate with the destination device at other end of the encrypted channel.

A MPLS Pseudowire connection was configured between a Cisco 7206 and a Cisco Catalyst 6509. A SITLine ETH encryption device was connected to each of the routers as a terminal device. We emulated customer Ethernet traffic by attaching a traffic generator to the user ports of the SITLine ETH. The SITLine ETH encrypted the traffic and sent it through the MPLS Pseudowire to the other end of the tunnel – replicating a real deployment scenario. We then verified that the traffic was encrypted between the two Cisco routers by monitoring the frames and confirming that they were illegible. Finally, we verified that no frames were lost in transit.

MPLS Pseudowire – RAW Mode Test Topology



Usage, Stability and Filters

MPLS Pseudowire – Tagged Mode

A second mode in which MPLS Ethernet Pseudowires can be configured is tagged mode. This mode of operation facilitates VLAN tagged traffic transmission across the Pseudowire. The routers facing the customer site expect to receive VLAN tagged traffic. In the event that the router receive plain Ethernet traffic, the router adds a VLAN tag for internal use. The tag is stripped from the Ethernet header before the transmission leaves the network for the receiving customer interface. Since the SITLine ETH is positioned between the customer switch and the provider router, the VLAN-tagged frames will be encrypted before entering the Pseudowire.

We verified that the SITLine ETH devices can establish secure connections through a VLAN-tagged MPLS Pseudowire. VLAN tagged Ethernet frames were sent through the secure connection without any loss being observed.

Handling of Bursty Traffic

Traffic rates within Carrier networks are usually not constant and vary according to changes in user behavior. These changes lead to traffic bursts which, for a short time, generate a higher load on the network and increase the stress on the devices providing connectivity. In these situations, the network devices must process a large amount of frames in a very short time and then return to normal operations.

We emulated bursty Ethernet traffic with a burst length of 101 and 301 Bytes in two tests scenarios to verify that the traffic bursts did not disrupt or disconnect the secure links between the SITLine ETH encryption devices. The SITLine ETH showed no signs of malfunction and no frame loss could be observed during this test.

Hardware Ethernet Frame Filter

The SITLine ETH has a built-in hardware-based filter that enables customers to define rules for the traffic that can be transported without encryption. For each line up to 12 filter rules can be configured. We set 12 different filter rules for each port directing the filters to allow the traffic to pass unencrypted. We verified that all filter rules worked perfectly as well as that no frames were lost when sending traffic close to line rate.

Ethernet OAM Transparency

Ethernet OAM frames are important for Carrier Ethernet services. Service providers use OAM to manage the customer edge devices and collect status messages to confirm that the customer edge device is operational. The frames are exchanged between the customer site and the provider edge device and have to be transmitted unencrypted.

We used the hardware filters to filter these OAM frames using the IEEE defined MAC destination addresses as filter rules. We verified that OAM frames, both for CFM (802.1ag) and EFM (802.3ah), were exchanged through the SITLine ETH devices without any problems.

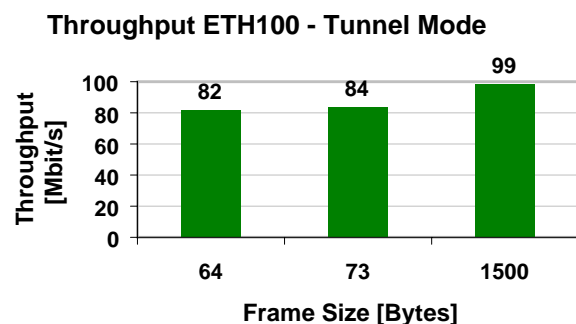
Long Term Stability

The SITLine ETH is expected to maintain encrypted connections between two points in a network over an extended period of time. In most cases, if the encrypted link is down, then the SITLine will declare the public port as down and no communication will be possible from one site to the other. We verified that the SITLine ETH is able to maintain a secure connection at 320 Mbit/s (80% line rate for 4-port device) over one hour without losing any traffic.

Performance

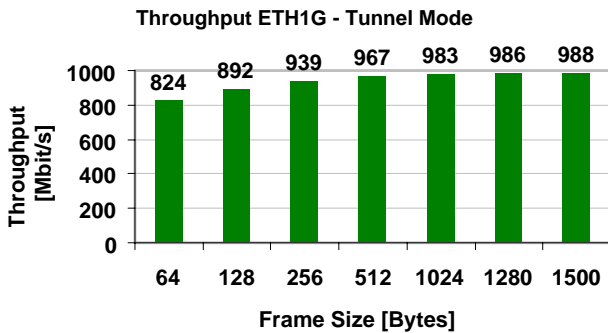
Ethernet Throughput

We tested the two variants of the SITLine ETH for performance: one with four Fast Ethernet ports; another with one Gigabit Ethernet port. Both variants support two operating modes that differ in the way the Ethernet traffic is encrypted or encapsulated. The tunnel mode requires an overhead of 18 Bytes for each Ethernet frame (14 Bytes Ethernet header + 4 Bytes Security Association Identifier – SAID). In the transport mode only the Ethernet payload is encrypted and the original Ethernet frame header remains untouched.

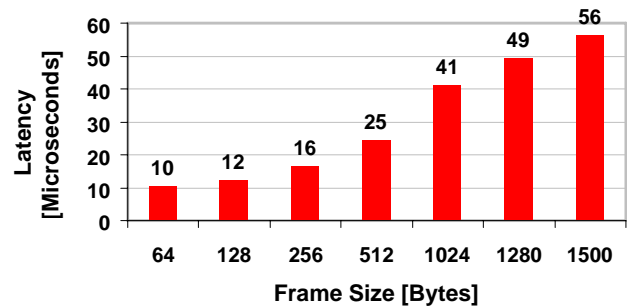


SITLine ETH100 – We measured the maximum loss-less Ethernet throughput according to RFC 2889 for both the transport and tunnel modes. In tunnel mode we achieved the theoretical maximum throughput performance after taking into account the additional Ethernet header of 14 Bytes and the SAID of 4 Bytes. The graph on page 3 shows the expected results from tunnel mode performance given the overhead required. In transport mode, we also achieved line rate throughput for all tested frame sizes.

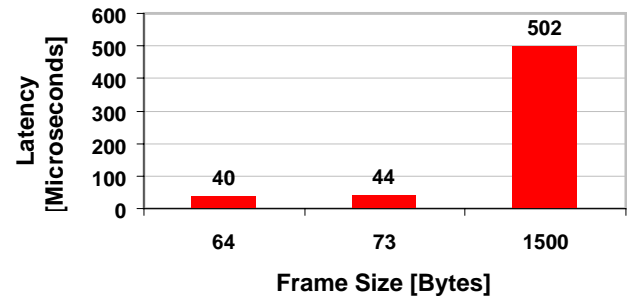
SITLine ETH1G – Again we measured the throughput for all frame sizes proposed in RFC 2889 for the Gigabit Ethernet solution. In transport mode as well as in tunnel mode we achieved the theoretical maximal throughput after taking into account the additional Ethernet header of 14 Bytes and the 4 Bytes SAID.



Latency ETH1G - Tunnel Mode



Latency ETH100 - Tunnel Mode



Latency

Customers require an encryption device that does not introduce latency to the Ethernet traffic. An increase in latency would affect realtime sensitive applications such as voice or video teleconferencing.

We measured the latency introduced by both SITLine ETH encryption devices. The latency depends on the frame size sent through the device because large frames require longer to pass through the device. We measured excellent latency values, well under one millisecond, even for large frame sizes such as 1518 Bytes. The following graphs show the latency values through both SITLine devices.

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/>