Rohde & Schwarz
R&S® SITLine ETH VLAN Encryption Device
Functionality & Performance Tests

Introduction

Following to our test of the Rohde & Schwarz SITLine ETH encryption device in April 2008 the European Advanced Networking Test Center (EANTC) continued the test series in 2009 with a new device generation which is called Rohde & Schwarz SITLine ETH VLAN. The Rohde & Schwarz engineers added support for multiple virtual connections per device port allowing the customer to use this device also for connecting several Virtual Private Network (VPN) sites with each other.

This device successfully passed the EANTC tests. We tested the performance, functionality, and security management capabilities of the new SITLine ETH VLAN device. The test results confirmed that the device is able to encrypt Ethernet traffic without impacting network performance.

Rohde & Schwarz SIT
R&S® SITLine ETH VLAN

- ☑ Ethernet Performance
  Nearly line rate throughput
- ☑ Robust Management
  Intelligent remote management
- ☑ MAC Learning
  MAC address learning

Test Period: July & September 2009

http://www.eantc.com

Tested by EANTC 2009

Test Highlights

- ➜ **Automatic Link Establishment**
- ➜ **Robust Security Management**
- ➜ **Nearly Line Rate Throughput**
- ➜ **Negligible latency by encryption device**
- ➜ **Scalability up to 4,000 Secure links**

Tested Devices & Test Equipment

Similar to the R&S SITLine ETH devices, two variants of the devices exist and were tested:

- 2-port Gigabit Ethernet device:
  SITLine ETH VLAN 1G
- 8-port Fast Ethernet device:
  SITLine ETH VLAN100

Each R&S SITLine ETH VLAN device is able to handle up to 4,000 different Secure Links using VLAN IDs according to IEEE 802.1q. For each VLAN ID a separate Secure Link is established to one remote encryption device. This allows the customer to setup several Secure Links from the same encryption device to different remote encryption devices sitting on different locations.

The devices support two encapsulation modes:

- Tunnel mode: The received Ethernet frames will be encrypted in their entirety and tunnelled using an additional Ethernet frame plus 4 Bytes Security Association Identifier (SAID)
- Transport mode: No additional overhead, only the payload is encrypted.

The devices can be operated in three network modes:

- EVPL: The devices are interconnected through an MEF defined Ethernet Virtual Private Line (EVPL) service. Each frame is assigned to a Secure Link based on different VLAN IDs tagged by the customer.
- MAC-EVPL: Like in the EVPL mode, the devices are interconnected through an MEF defined EVPL service. Different to the EVPL mode, each frame is assigned to Secure Links based on the destination MAC address. The encryption device is managing a MAC address table and adds an appropriate VLAN ID to each frame based on the information stored in the MAC address table.
- MAC-ELAN: The devices are interconnected through an MEF defined Ethernet LAN (ELAN) service. Each frame is assigned to Secure Links based on the destination MAC address. VLAN tagging is not needed as the ELAN service takes care of delivering the frames to the destination.

Our test environment was based on an MPLS network containing three MPLS provider edge (PE) routers with appropriate pseudowires configured. The achieved results can also be adopted to any other transport technology providing Ethernet tunnel mechanism as the Rohde & Schwarz SITLine ETH VLAN does not rely on a specific backbone technology.

Functionality in EVPL Mode

In this set of tests we verified the Rohde & Schwarz SITLine ETH VLAN ability to connect between multi-point connected sites and its auto configuration and recovery features.

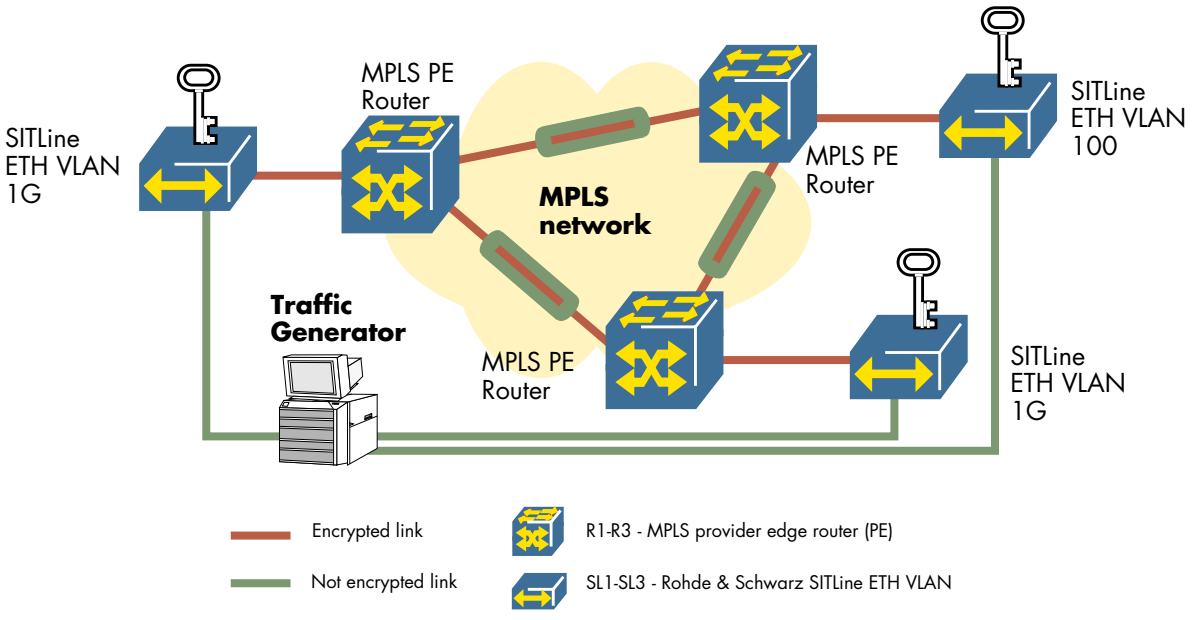
Test Highlights

- ➜ Automatic Secure Link Establishment
- ➜ Recovery of Secure Links
- ➜ Automatic VLAN ID Scanning
- ➜ Device Redundancy Without Service Interruption

Automatic Secure Link Establishment

In some cases traffic was not sent all the time between two VPN sites. Rohde & Schwarz had implemented a function in which the encryption devices are able to establish Secure Links on demand as soon as frames for a specific VLAN arrive at the user port. The operator can configure the VLAN ranges that are allowed to operate in this 'on-demand' mode. The challenge for the encryption device is to identify the frames with VLAN IDs that are not currently used for running Secure Links and to establish new Secure Links for the detected VLAN ID.

The Rohde & Schwarz SITLine ETH VLAN device was able to establish Secure Links on demand with establishment times between 74 and 160 milliseconds.



This means for the customer to be able to setup Secure Links whenever they are needed without having a long establishment delay.

Recovery of Secure Links

VPN devices rely on a stable backbone connection. When backbone links fail, the customer normally expects some resiliency mechanisms to be implemented in the backbone and indeed most (if not all) service providers design their backbones to be highly resilient.

An encryption device such as the Rohde & Schwarz SITLine ETH VLAN must be able to automatically reconnect and reestablish encrypted links after a failed backbone connection returned back to operational state. Both SITLine ETH VLAN devices belonging to one Secure Link send Secure Link Check (SLC) messages once a minute to check to verify connectivity to the remote device.

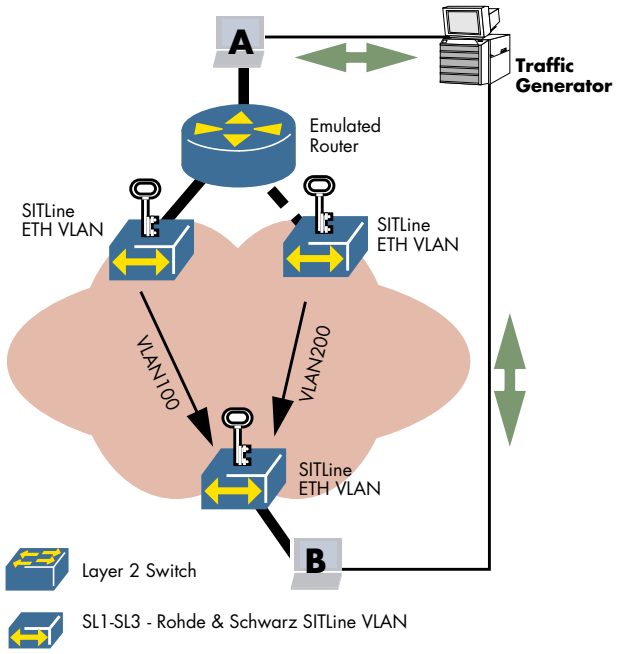
In our test the Secure Links were not influenced in any way when the out of service time in the backbone was less than the SLAC message interval.If the backbone out of service time is greater than 60 seconds (the SLC interval), the Rohde & Schwarz ETH VLAN deactivated the Secure Link and reestablished it within the next SLC interval after the backbone connection was up again. The customer do need to care about that his secured connections need to be re initialized after a backbone failure, this is done automatically.

VLAN ID Scanning

Each Rohde & Schwarz SITLine ETH VLAN device tries to find SITLine devices at the other end of the network by sending special discovery messages through all VLAN IDs, this is called VLAN ID scanning. We verified, that this procedure automatically finds configured - pseudowires. This is used by the SITLine devices to find each other in the network. This feature simplifies the SITLine network deployment as the devices just need to be activated without the burden of configuring the services manually.

Redundancy

The SITLine ETH VLAN devices support redundant locations. If a customer is connecting one of its locations through two different SITLine ETH VLAN devices (e.g. using two Internet service providers) for redundancy purposes, the SITLine ETH VLAN devices are providing a redundancy mechanism.



We emulated a switchover within the network and successfully verified that the SITLine ETH VLAN device was able to handle the switchover without introducing an additional failover time.

Performance Tests

In order to show that customer will not see a decrease of performance while putting the SITLine devices in their network, we performed several performance tests showing excellent results.

Test Highlights

- ➜ Nearly Line Rate Throughput
- ➜ Very Low Forwarding Latency
- ➜ Up to 4,000 Secure Links in Parallel

Both variants of the Rohde & Schwarz SITLine ETH VLAN device participated in our performance tests:

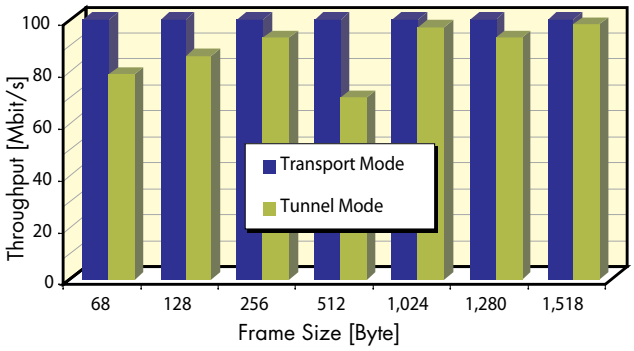
- the SITLine ETH VLAN 1G solution with one Gigabit Ethernet pair
- the SITLine ETH VLAN 100 solution with four Fast Ethernet pairs

Throughput

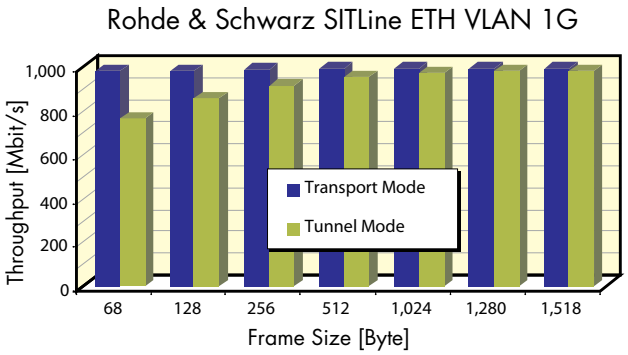
We tested both variants of the device in transport mode and in tunnel mode. The SITLine ETH VLAN device showed nearly line rate if the device was configured to use the transport mode.

While running the device in tunnel mode an additional header decreased the theoretical maximum throughput accordingly. In our tests the measured throughput was in most cases near to the expected theoretical maximum.

Rohde & Schwarz SITLine ETH VLAN 100



Rohde & Schwarz SITLine ETH VLAN 1G

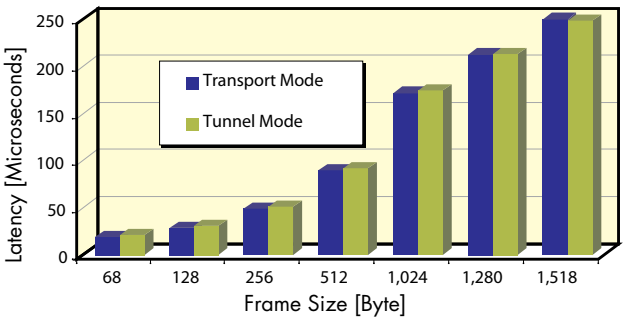


Latency

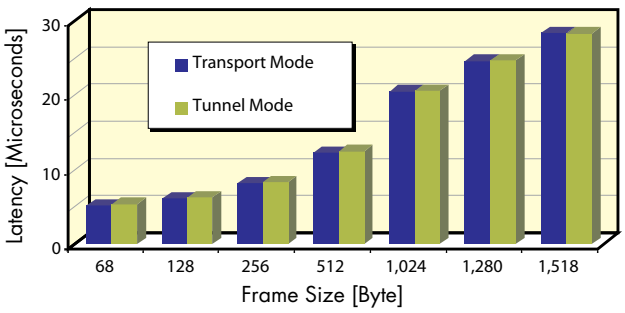
As realtime sensitive applications such as voice or video transmission require low latency, such an encryption device like the Rohde & Schwarz SITLine ETH VLAN must not introduce an significant amount of additional latency to the network.

The Rohde & Schwarz SITLine ETH VLAN devices showed excellent latency values, well under one millisecond, even for large frame sizes such as 1,518 Bytes. The following graphs show the latency values through both SITLine devices.

Rohde & Schwarz SITLine ETH VLAN 100



Rohde & Schwarz SITLine ETH VLAN 1G



Scalability of Secure Links

The idea behind the SITLine ETH VLAN device running in VID-EVPL mode is to have at least one VLAN based point-to-point connection for each potential remote location configured in the core network. The customer is not limited to use only one VLAN ID per remote location. He could also use several point-to-point connection to the same remote location, for instance to separate different VPNs.

The Rohde & Schwarz SITLine ETH VLAN encryption device is able to support several Secure Links per port each using different VLAN IDs. According to the device specification up to 4,000 different Secure Links are supported on each device, either all on one port or spread throughout all used ports.

Each SITLine device was able to handle up to 4,000 Secure Links. Even with 4,000 Secure Links activated, the throughput and latency performance did not decrease significantly.

Security Management

Each Rohde & Schwarz SITLine ETH VLAN device needs access to the SITScope Security Management Server (SMS). The SMS controls all security settings of each device like encryption scheme, Secure Link configurations and encapsulation. We tested the functionality and the reliability of the SMS implementation.

Test Highlights

- ➜ Remote Management Autodetection
- ➜ Very Low Forwarding Latency

Remote Management

The Rohde & Schwarz SITLine ETH VLAN devices are able to access the SITScope Security Management Server (SMS) either via the LAN connection or remotely using inband management. If one of the Rohde & Schwarz SITLine ETH VLAN devices itself does not have local connection to the SMS, it searches for other SITLine ETH VLAN devices in the network which have local access to the SMS.

In case of remote management the MAC frames used to transmit management traffic are encapsulated into another MAC frame (MAC-in-MAC or Provider Backbone e Bridges according to IEEE 802.1ah) and transported over the same pseudowire (same VLAN ID) as the Secure Link (inband management).

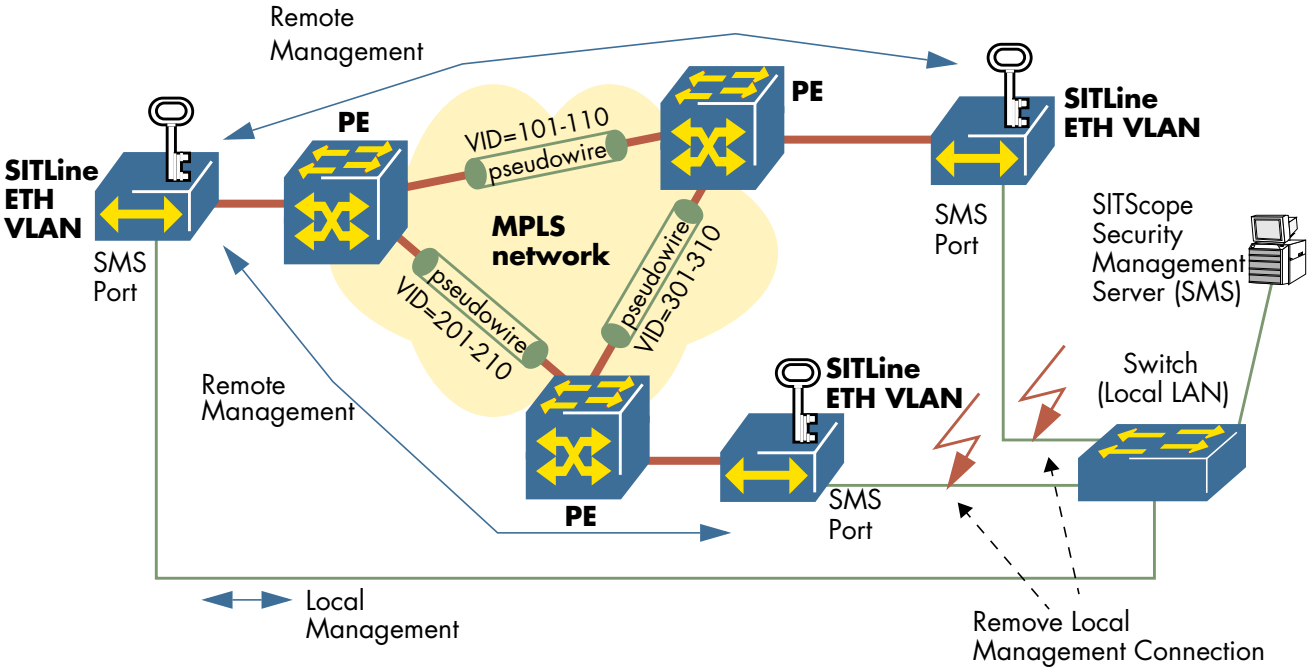
After cutting the local management access of one SITLine ETH VLAN device, it detected that it lost local connection to the SMS and automatically searched for alternative devices in the network with local access to the SMS. The device which lost the local connection to the SMS established a remote management session to the SMS through the remote SITLine ETH VLAN device which had local access to the SMS. Even after the Secure Links were disabled the SITLine devices were still able to access the SMS.

For the customer this is a major security and resiliency aspect as the SMS will still be accessible even if some local connection to the SMS will fail.

Robustness of Remote Management

Each Rohde & Schwarz SITLine ETH VLAN device uses only one VLAN to establish an remote connection to the SMS.

Our test showed that the SITLine devices are able to reestablish remote management connections using different pseudowires if the one they are currently using failed.



SITLine ETH VLAN in MAC Mode

Besides the VLAN-EVPL mode the SITLine ETH VLAN devices support two additional modes:

- MAC-EVPL mode
  SITLine ETH VLAN devices are interconnected to each other through VLAN based point-to-point layer 2 tunnels like MPLS pseudowire; the customer does not need to set appropriate VLAN IDs as this is done by the SITLine ETH VLAN devices according to the MAC destination address of each frame which previously was learned by the remote device and propagated to all other devices in the network
- MAC-ELAN mode
  All SITLine ETH VLAN devices are interconnected through a layer 2 VPN like the MEF defined E-LAN service; the SITLine ETH VLAN devices choose the correct Secure Link according to the previous learned MAC addresses

Test Highlights

➜ MAC Learning

➜ No VLAN Configuration Needed at the Customer

➜ Support for MEF Defined E-LAN Service

The main difference to the VID-EVPL mode is that the customer does not need to configure and set VLAN IDs for each of its connected remote locations. Running the SITLine ETH VLAN device either in MAC-EVPL mode or in MAC-ELAN mode, it learns the MAC addresses of the hosts located in the secured customer network and automatically chooses the appropriate Secure Link based on the learned MAC addresses.

We verified the functionality for both modes.

MAC-EVPL Mode

Running the SITLine ETH VLAN device in MAC-EVPL mode, the customer does not need to care about any VLAN configuration. The SITLine ETH VLAN devices are learning the MAC addresses from the local connected hosts and inform all other connected SITLine ETH VLAN devices about the learned addresses (remote learning). The SITLine ETH VLAN devices auto–matically adding the appropriate VLAN ID in order to reach the desired location.

In MAC-EVPL mode the SITLine ETH VLAN device is able to learn 256 remote MAC addresses. For each neighbor SITLine (which it detects via VLAN ID scanning) it establishes one secure link.

By sending all frames without VLAN Tag we verified the correct operation of this mode. The SITLine ETH VLAN device added the appropriate VLAN Tag according to the entry learned in its MAC address table and forwarded the frames within the corresponding Secure Link.

MAC-ELAN Mode

In contrast to all other modes, the SITLine ETH VLAN device does not require point-to-point connections between all the locations if running the device in MAC-ELAN mode.

In MAC-ELAN mode the SITLine ETH VLAN device is able to learn MAC addresses. It chooses the appropriate Secure Link according to the MAC entries in its MAC address table. This mode is intended to give the customers the possibility to use the SITLine ETH VLAN devices to encrypt their traffic running through an MEF defined E-LAN service.

Our test showed that the SITLine ETH VLAN device is able to learn MAC addresses of hosts connected to remote locations.

The Rohde & Schwarz SITLine ETH VLAN device showed its ability to learn MAC addresses in MAC-ELAN mode and the capability to encrypt and forward Ethernet traffic accordingly. The SITLine ETH VLAN device did not flood or drop frames

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/