NewSONET/SDH – Ethernet Interworking Testing with the ONT-503/506/512

Interworking verification of Ethernet over SONET/SDH (EoS) systems

NewSONET/SDH systems allow for more flexible utilization of available bandwidth over legacy SONET/SDH networks, allowing for the optimal transmission of widely differing data services having different bandwidths. The latest NewSONET/SDH network elements offer capabilities for a wide variety of tributary services, including Ethernet and Fiber Channel in addition to the line interfaces, and integrate switching and cross-connects in the various layers. The add/drop multiplexers of the past have now become complex multi-service provisioning platforms (MSPPs).

Different tests for each of the different technologies must be performed for verification of NewSONET/SDH network elements.

Ethernet over SONET/SDH (EoS) is the focus in this application note.

Verification of EoS systems involves testing in two specific areas. First, all of the functions of the SONET/SDH line side are tested, including the SONET/SDH interface, virtual concatenation, differential delay, LCAS, GFP, and MAC/Ethernet (Figure 1). In each case, a loop is switched into the appropriate layer of the network element (pre-GFP, pre-Ethernet, or Ethernet) for this purpose. The test set stimulates various situations in the corresponding technology and verifies that the network element responds with the expected reaction to the stimulus.

It should be noted that some restrictions in the completeness of the tests must be accepted, as the loopback mode behavior of the network element may differ from the behavior in Through mode.

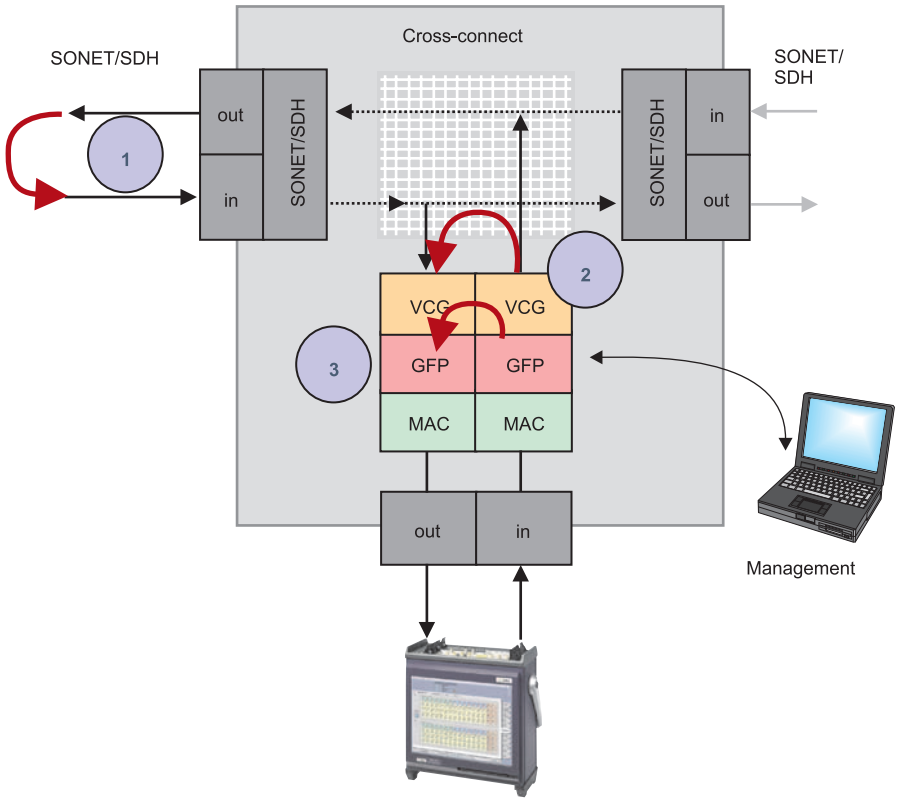

Figure 1: Verification of the NewSONET/SDH side using DUT internal loops.

Second, transmission of Ethernet traffic over NewSONET/SDH is verified using an Ethernet tester (Figure 2). A loop is switched into the SONET/SDH line side for this purpose. Ethernet traffic using various formats (VLAN, LLC, ...), various

loads (0-1 Gb/s), various frame lengths (from minimal up to jumbo length), and various traffic profiles (burst or constant), is measured.

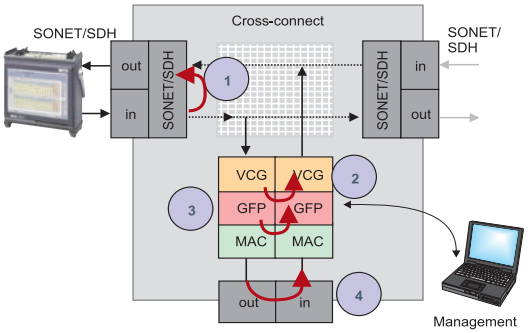

Figure 2: Verification of the Ethernet-side using DUT internal loops.

These test scenarios allow for the testing of the main functions of the MSPPs, but they do not test the interworking between Ethernet and NewSONET/SDH.

Why perform interworking testing?

Interworking testing measures the reactions of a network element on the SONET/SDH side caused by various Ethernet situations in the tributary (and vice versa). In addition, it also verifies that the technologies operate together without any errors. Interworking testing requires interaction between the NewSONET/SDH tester and the Ethernet tester. It cannot be achieved using the traditional loopback operation. The JDSU ONT-503 allows for interworking verification of EoS systems using one instrument (Figure 3).

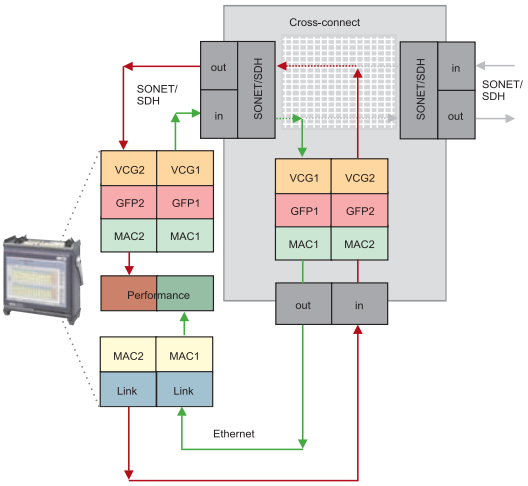

Figure 3: Interworking with the ONT-503.

Several interworking test scenarios are described below (Abbreviations used: NST = NewSONET/SDH tester, DUT = device under test, ET =Ethernet tester)

Asymmetrical VC groups (with LCAS) and Ethernet traffic

Ethernet traffic in the forward and return paths of real systems is not necessarily the same. It may be asymmetrical with respect to bandwidth, frame length, and profile. Similarly, the VC group (VCG) size does not have to be the same in the forward and return paths. These two observations result in new situations for network element testing that cannot be verified using either an end-to-end Ethernet tester or a VC loop (Figure 4).

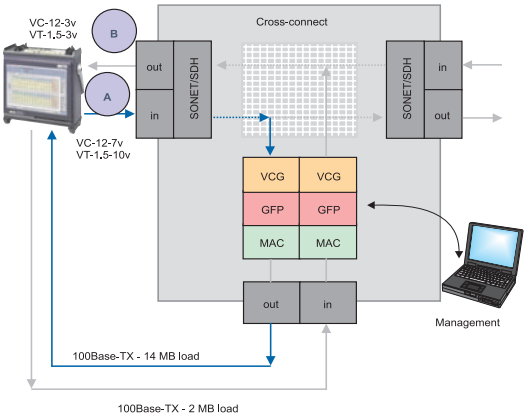

Figure 4: Asymmetrical VCGs and Ethernet traffic.

Consider the failure of the SONET/SDH path on one side:

Path "A" must remain fully in service if path "B" fails. The LCAS source of path "A" stores the last returned status of path "B" (MST) and retains it. Path "A" continues transmitting Ethernet traffic. If path "B" service is restored, then there is no effect on path "A".

Generating and detecting GFP CSF alarms

Client signal fail (CSF) alarms are generated in the GFP layer of the DUT (Figure 5). They are triggered by malfunctions in the physical Ethernet interface or link, and they are transmitted in GFP over SONET/SDH.

The cause of this alarm is often "no light" or too high an offset at the Ethernet port on the physical interface, resulting in the loss of client signal (LOCS). In addition, high error rates from code, disparity, and bit errors can generate a loss of client character synchronization (LOCCS) on the link.

If a CSF alarm is detected in the return path of the GFP layer, some implementations will shut down the link. Other interactions between GFP and Ethernet, OAM functions for example, are currently being standardized by the Metro Ethernet Forum (MEF) and by the ITU-T in the draft entitled "Y.ethoam".

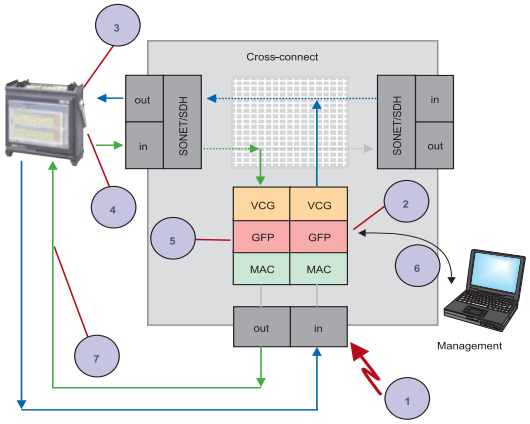

Figure 5: Client signal failure (CSF) alarms .

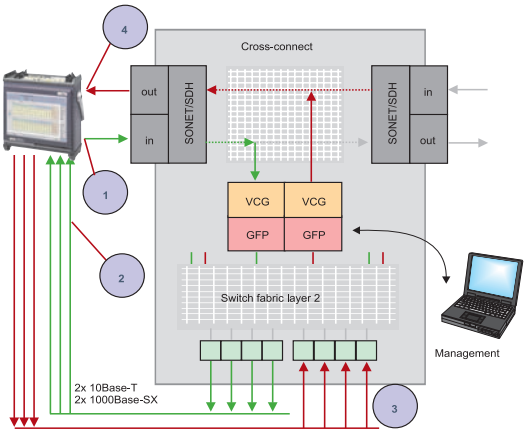

Figure 6: Verification of transfer delay (latency).

Blue path: ET generates Ethernet errors (1), DUT generates CSF (2), and NST detects correct CSF (3)

Green path: NST generates CSF in GFP (4), DUT detects CSF (5), monitoring by management system (6), DUT shuts down the link, and ET detects the down link (7)

Determining transfer delay (latency)

The determination of transfer delay is performed mainly to ensure minimal delay times for time-sensitive services such as voice and video transmissions. Similarly, Ethernet traffic flow control is only possible if the delay times are not too high.

Latency can increase sharply when high traffic loads occur, leading to the "rejection" of frames or the loss of data packets. When the traffic stress condition ends, though, it is necessary to ensure that shorter delay times are again achieved. In addition, this process must b e reproducible. Traditional loopback measurements do not allow for testing using the limited operations of this practical situation (Figure 6).

Green path: NST transmits timestamp in mapped Ethernet (1) and ET detects timestamp and measures transfer delay (2). Red path: ET transmits timestamp in Ethernet signals (3) and NST detects timestamp in mapped Ethernet and measures transfer delay (4).

Delay measurement requires time synchronization of the ET and NST. The most effective solution is to have the ET and the NST in the same instrument.

Flow control emulation on the Ethernet link and in SONET/SDH

Flow control was developed to prevent loss of data during excessive traffic loads. This mechanism generates pause frames in the return path, which cause the transmitter to reduce traffic in a controlled manner until the corresponding receiver is again able to receive and transmit again without errors. Flow control takes place in the MAC layer on Ethernet links in the same way as with mapped Ethernet on SONET/SDH links.

For this reason, the flow control on both the Ethernet and the SONET/SDH sides of the DUT must be tested. To perform this test, the switch in the DUT is increasingly loaded with traffic until it reacts with pause frames in the SONET/SDH MAC or Ethernet MAC direction. The pause actions as well as the expected error-free Ethernet traffic are then measured (Figure 7).

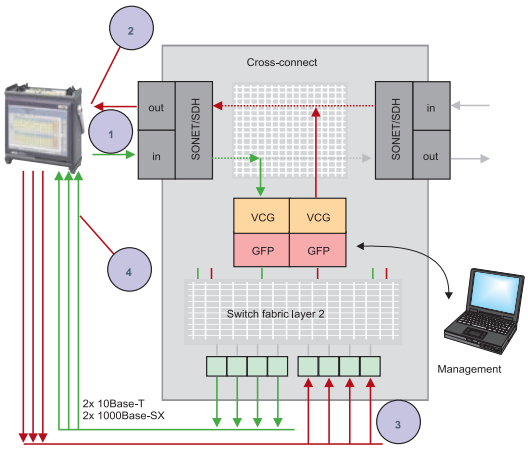

Figure 7: High loads in the switch matrix cause flow control of MAC traffic in Ethernet and SONET/SDH links.

Green path: NST transmits Ethernet traffic (1) and the switch reacts with pause frames in mapped Ethernet due to overloading (2). Red path: ET transmits traffic (3) and the switch reacts with pause frames due to overloading (4).

Ethernet coding verification using a pseudorandom bit sequence (PRBS)

All Ethernet interfaces transmit data using specific coding procedures. These codes are generated in the Ethernet transmitter, are decoded by the receiver, and are mapped as traffic in GFP and SONET/SDH. A "continuous" PRBS that generates all possible data pattern combinations, and hence all possible coding situations, is inserted into the payload of the Ethernet frame to ensure that coding and decoding is always performed correctly. The error-free behavior is verified by a bit error rate (BER) increment in the payload.

Interworking requirements for test instruments

The MAC traffic payload in the NewSONET/SDH tester and the Ethernet tester must be identical in order to analyze the traffic fed into the Ethernet port of a DUT with a NewSONET/SDH tester connected to it. However, all Ethernet testers and NewSONET/SDH testers have manufacturer-specific Ethernet payloads. Normally, a test frame containing a timestamp for transfer delay (latency) tests and a sequence number for throughput measurements (lost frames), is provided in the payload (Figure 8). Currently, there is no standard for these test frames. Each manufacturer of test equipment defines their own specific test frame.

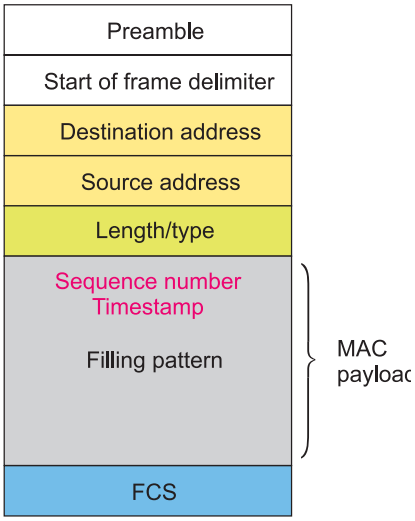

Figure 8: Ethernet MAC test frame with timestamp and sequence number.

The ONT-503 includes a NewSONET/SDH module and an Ethernet module that work with the same Ethernet test frames. This is the only test solution to ensure that all of the requirements are met for interworking verification of EoS systems.

Test & Measurement Regional Sales

NORTH AMERICA
TEL: 1 866 228 3762
FAX: +1 301 353 9216

LATIN AMERICA
TEL:+55 11 5503 3800
FAX:+55 11 5505 1598

ASIA PACIFIC
TEL:+852 2892 0990
FAX:+852 2892 0770

EMEA
TEL:+49 7121 86 2222
FAX:+49 7121 86 1222

WEBSITE: www.jdsu.com