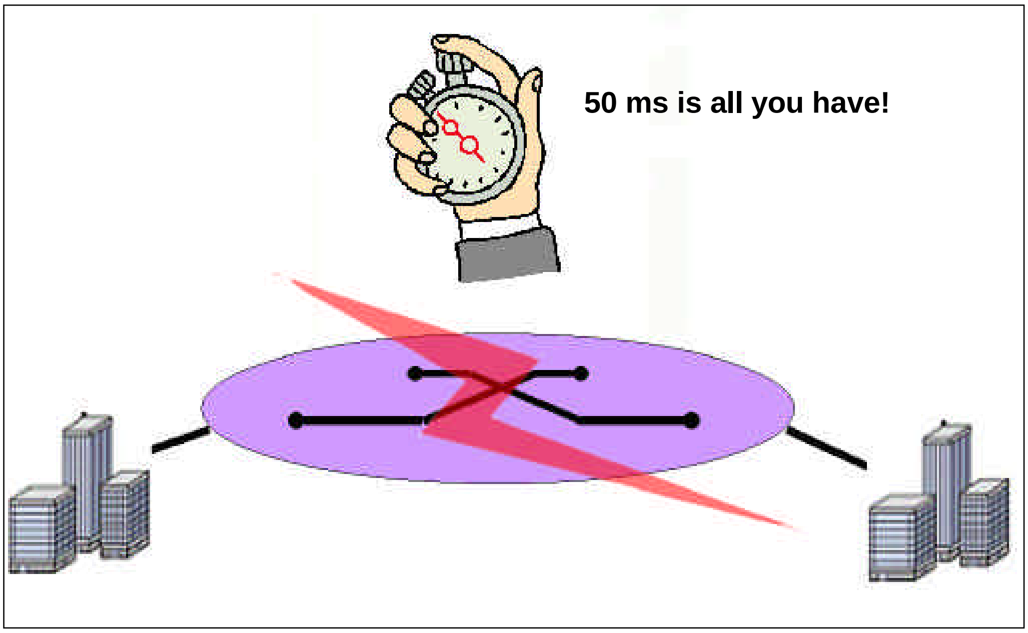
Measuring APS Disruption Time

TABLE OF CONTENTS:

SONET and SDH networks are monitored by special mechanisms involving Bit Interleaved Parity (BIP) controls. These mechanisms are designed to sectionnalize and identify the nature of the problems but they do not solve them.
That is why another protection mechanism has been defined in order to guarantee the availability of the network in case of problems. Its name is APS=Automatic Protection Switching



There are two aspects in APS:

- Protocol aspect (information exchange between network equipments)
- Switch time reaction (time it takes for the network to complete the protection switch)

This application note is focused on the second aspect : how to measure the APS disruption time.

The first part of this document describes the different APS architectures.

The last part describes how you can benefit from the CMA 5000 OTA Application capabilities for performing easy and accurate APS switch time measurement.

1.0 What is APS (Automatic Protection Switching) ?

Due to the large amount of information being transferred over Synchronous Optical Network (SONET/SDH), there are considerable financial stakes involved and it is therefore vital to ensure that the transport services are as readily available as possible.
So, protection mechanisms are implemented in order to prevent long disruption times in the case of failure.
In its simplest form, SONET/SDH protection is based on the implementation of alternate paths for traffic divided between the working portion of the network and the protected portion of the network.
Generally speaking, APS involves switches of a redundant path both at the transmitter and at the receiver levels.
The term "Bridge" is used for the selection of the transmit path.
The term "Selector" or "Switch" is used for the selection of the receive path.

There are many solutions to the problems that can affect SONET/SDH equipment (equipment failures, mechanical failures). While all the solutions involve some use of redundant transmission systems, they can be found in a number of network configurations. These physical configurations include:

- **Linear protection (between 2 points)**
- **Ring based protection**

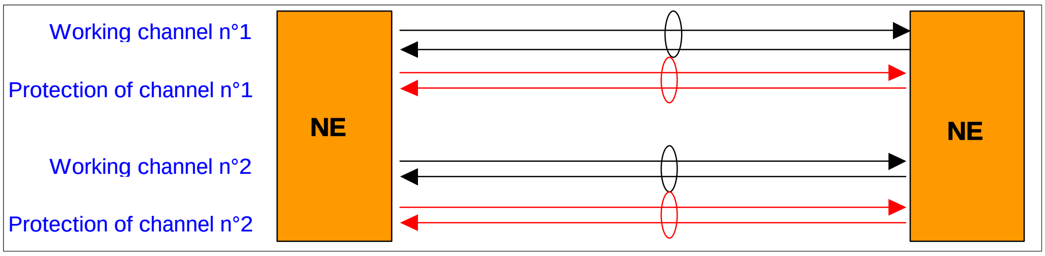
The principles and protocols of APS are identical for SONET and SDH. They are defined in the following recommendations:

- **SONET:** GR-253 Core issue 3
  GR-1230-Core (Bidirectional Line-Switched Ring equipment Generic Criteria)
  GR-1400-Core (Dual-Fed Unidirectional Path Switched Ring)
- **SDH:** G.783 (Characteristics of synchronous digital hierarchy (SDH) equipment functional blocks).
  G. 841 (Types and characteristics of SDH network protection architecture).

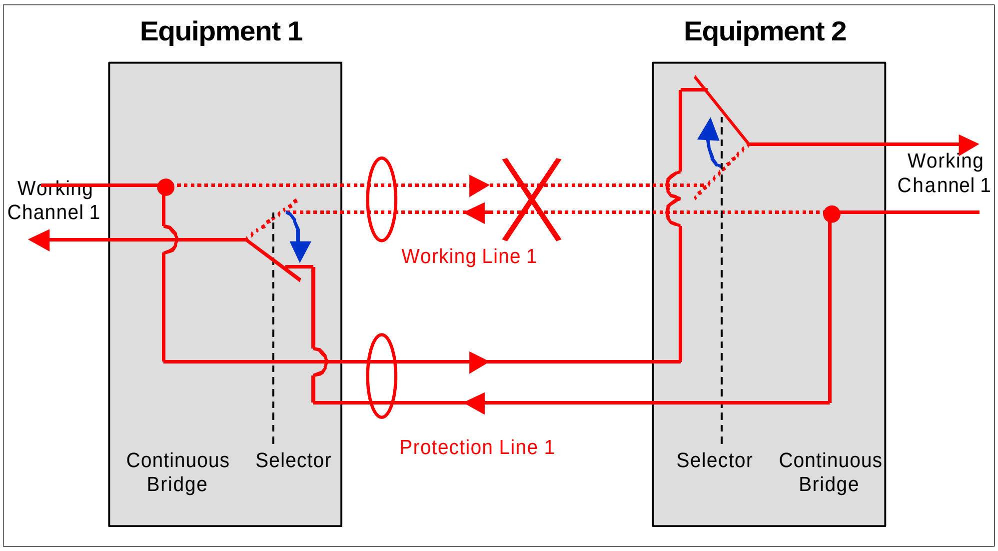
1.1 Linear protection

Two linear protection architectures are defined: 1+1 Architecture
1: n Architecture

1+1 Architecture



In 1+1 architecture, each channel has a dedicated protection channel.
It is the most redundant solution.

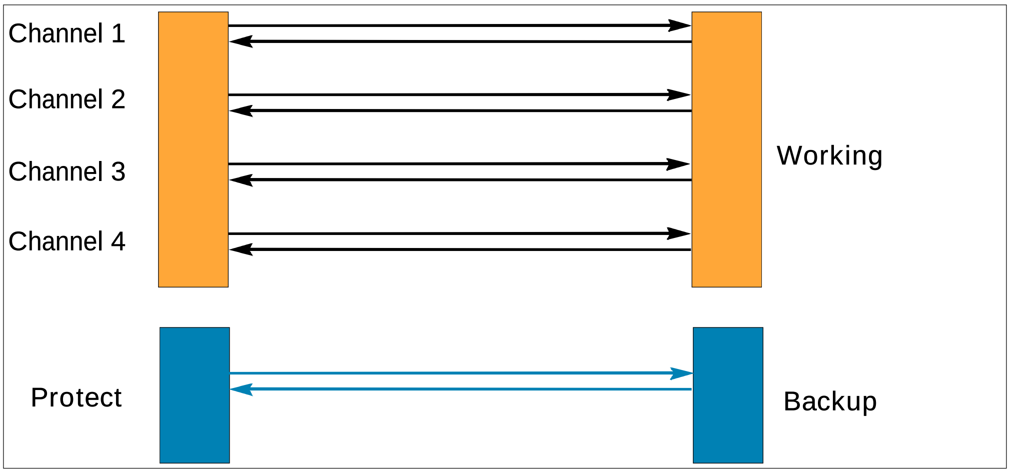


Linear APS Switch - 1+1 Architecture

In short, the 1+1 architecture is an architecture in which the head-end signal is continuously bridged. So, the signal is simultaneously transmitted on the working channel and the protection line.
By default, the 1+1 architecture is:

- Unidirectional (only the channel in the failed direction is switched to the protection line)
- Nonrevertive (in nonrevertive switching, a switch to the protection line is maintained even after the working line has recovered from the failure that caused the switch).

1:n Architecture



Linear APS Switch - 1:n Architecture

It is an architecture in which any of the “n” working channels can be bridged to a single protection line. Every channel shares the same protection channel.

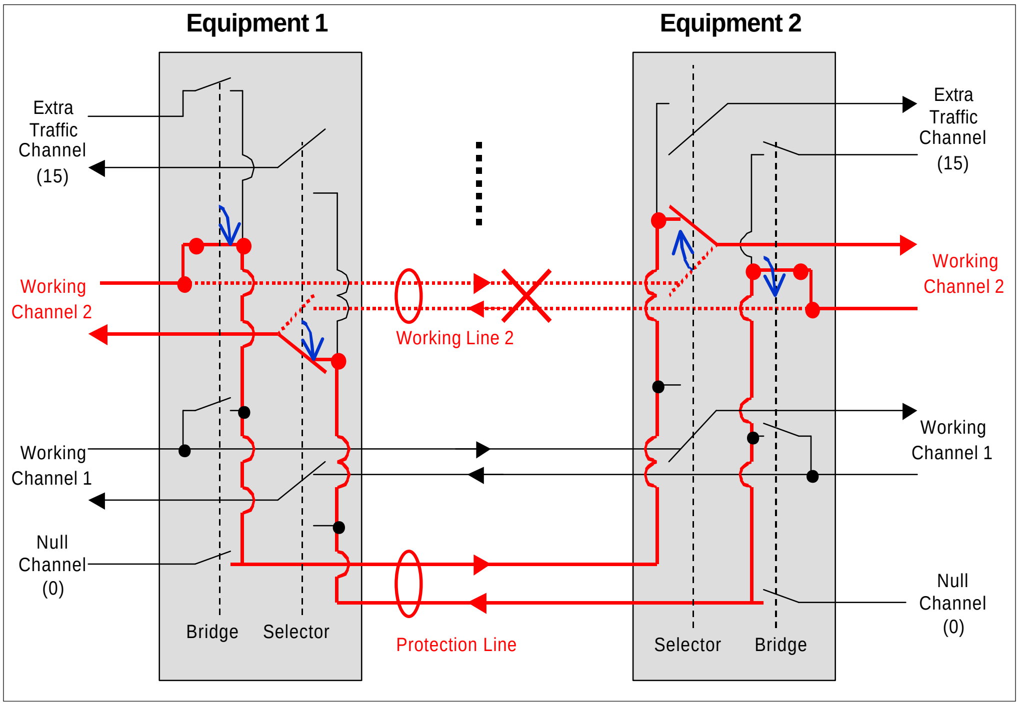
Permissible values of “n” are from 1 to 14.

Because the head end is switchable, the protection line can be used to carry an extra traffic channel.

By default, the 1:n architecture is:

• Bidirectional: in this mode, a channel is switched to the protection line in both directions.

• Revertive: in revertive switching, the traffic is switched back to the working line when the working line has recovered from the failure.



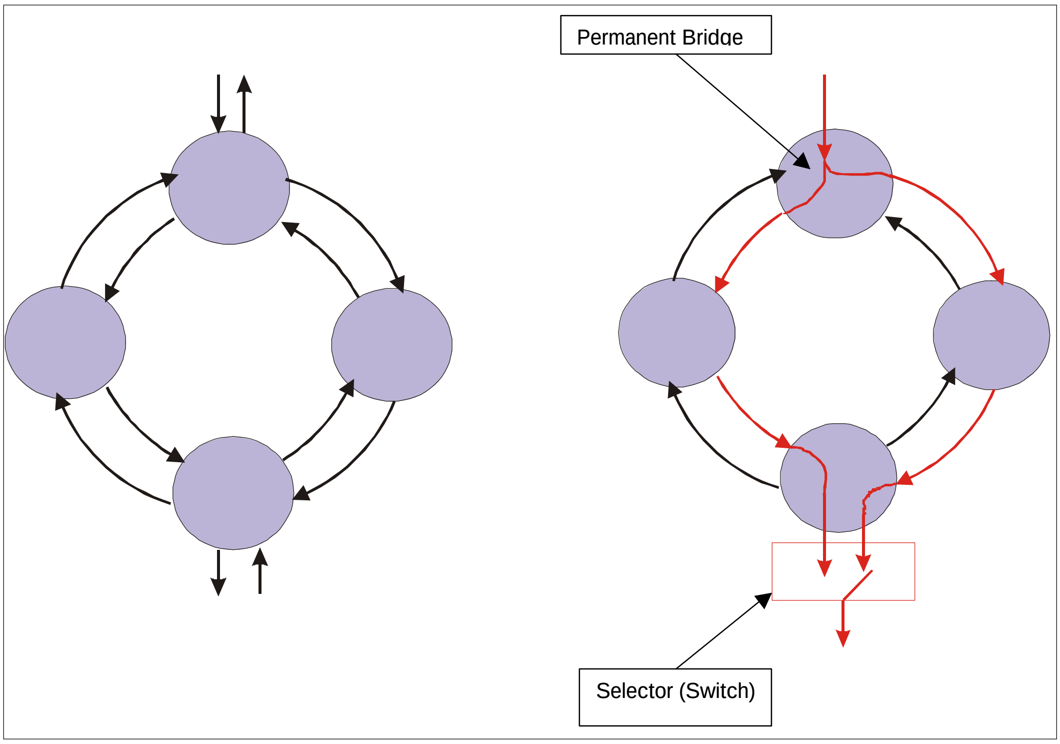
Linear APS Switch - 1:n Architecture

1.2 Ring Based Protection

Subnetwork Connection Protection (SNCP) and Multiplex Section Shared Protection (MS-SPRing)

SNCP

SNCP performs path protection switching (called dedicated protection) which manages all traffic by a path. Working traffic is transmitted in one direction, protection traffic in the opposite direction around the ring, and traffic is selected at each end of the path. So, SNCP supports multiple rings, and offers suitable solutions for access and metro networks where hub nodes terminate most various traffics.



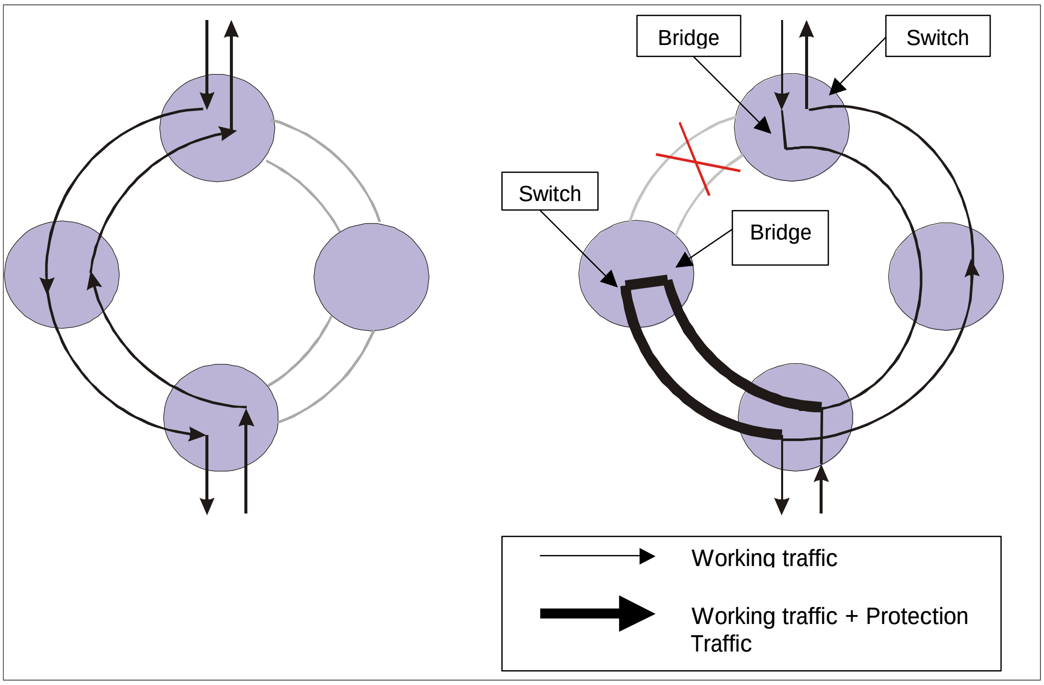
SNCP

MS-SPRing

MS-SPRing performs ring switching or span switching between nodes. All the working traffic and protection traffic is transmitted bidirectionally over spans. The protection traffic can be flexibly used for extra traffic, not protection.

2F MS-SPRing

Each fiber handles both working traffic and protection traffic, and half of the bandwidth can be used for working and the remainder for protection, thus protecting the working traffic transmitting in the opposite direction around the ring. Traffic is terminated at each node around the ring, so 2F MS-SPRing can reuse the bandwidth and provide an effective networking solution.



2F MS-SPRing

2.0 APS Protocol for Linear and Ring Architecture

2.1 Switch Initiation Criteria

The network must activate the APS protocol when a “default” occurs.
There are two automatic switch initiation criteria:

- Signal Fail (SF): it is a “hard failure” condition detected on the incoming STM-N/OC-N signal:

  Loss of Signal (LOS)
  MS-AIS/AIS-L alarm
  and BER exceeding 10E-3 on the incoming STM-N/OC-N signal.

- Signal Degrade (SD): it is a “soft failure” condition. When the BER exceeds a pre-selected threshold, the APS controllers detect an SD condition on that line. The BER threshold for an SD condition is user-provisionable over the range of 10E-5 to 10E-9.

2.2 APS Channel Protocol

The APS protocol for both architectures (Linear and Ring) is carried by K1 and K2 bytes.
The APS controllers use these two bytes to exchange requests and acknowledgements for protection switch actions.
K1 and K2 are used to indicate bridging and switching actions.
However, the bit assignments for K1 and K2 bytes are different depending on whether you have a linear architecture or a ring architecture.

The protocol aspects are described in the application note “Validate APS protocol with CMA 5000 OTA”.

2.3 Switch Completion

The protection process involves “Bridge” actions (optionally) and “Switch” actions.
This process is completed when the equipments at both ends have completed “Bridge” and “Switch” actions within the same 50 ms completion time.
The result of this operation is the disappearance of the defaults because the traffic is then transmitted on the protection channel.
There is optionally a last action: restoral and clearing of SD and SF condition.
This action depends on whether the network uses revertive or non-revertive switching.
In revertive switching, the traffic is switched back to the working line when the working line has recovered from the failure.
A clearing method is defined in the recommendations based on BER detection on the working channel under repair.

3.0 Network Objectives

During a switch, the traffic is interrupted and many defaults may appear (alarms, errors,...) and may cause degradation of the transmission performance or unavailability of the link.

From the operator’s point of view, the most important parameter to consider is the switch time.
The time to complete a switch, once it is initiated, must be 50 ms or less as defined in both ITU-T G.783 and Bellcore GR-253.
This objective is the same for both architectures: Linear and Ring.

4.0 Measuring APS Disruption Time with CMA 5000 OTA

As mentioned above, one of the main APS parameters is the switch time. This switch time should not take more than 50 ms (according to the Bellcore/ITU-T recommendations).

CMA 5000 OTA is able to detect the defaults that may appear during a protection switch and display their duration with 125 µs resolution. With CMA 5000 OTA, you can see at a glance if your network complies with the objective defined by the recommendations and much more!

With the “Event Analysis” function of CMA 5000 OTA, you have access to all the information from a single window: total switch duration, details of all the events, partial duration for each event...

This is the crucial advantage of CMA 5000 OTA in relation to its competitors that generally follow only one parameter to measure the switch duration.

4.1 Measurement Principle

The 5 steps of APS disruption time measurement as follows:

- **Connect OTA module to the network**
- **Configure OTA application**
- **Generate defaults in the network in order to initiate the protection process** [1]
- **Read the results in “Duration” window**
- **Save the results.**

The 5 steps are described individually in the following paragraphs.

Notes:

[1] For this action, we use a second CMA 5000 OTA unit configured in Through Mode in order to be able to generate calibrated defaults and cover all SF and SD condition criteria

4.2 Connecting CMA 5000 OTA to the Network

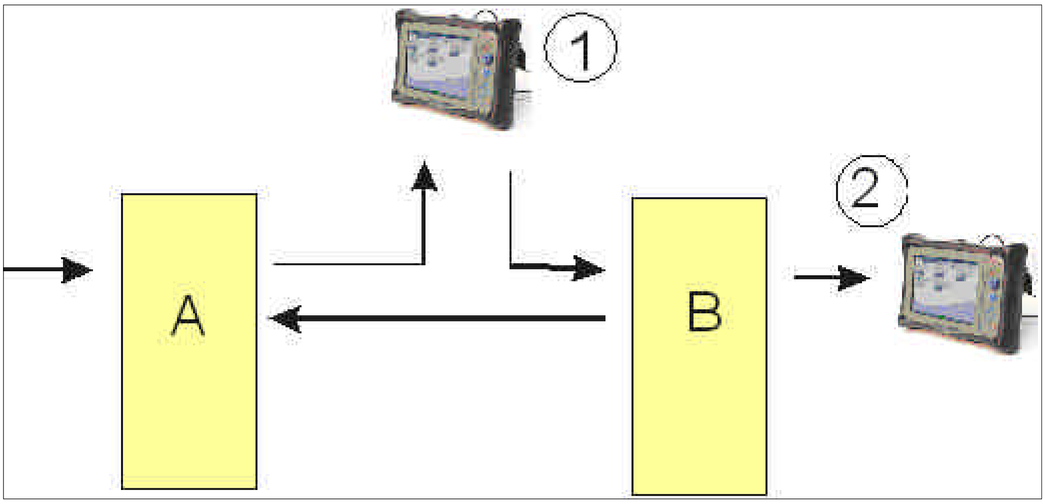
As described above, we use 2 CMA 5000 OTA:

- the first for generating defaults and initiating the protection process (shown as number 1)

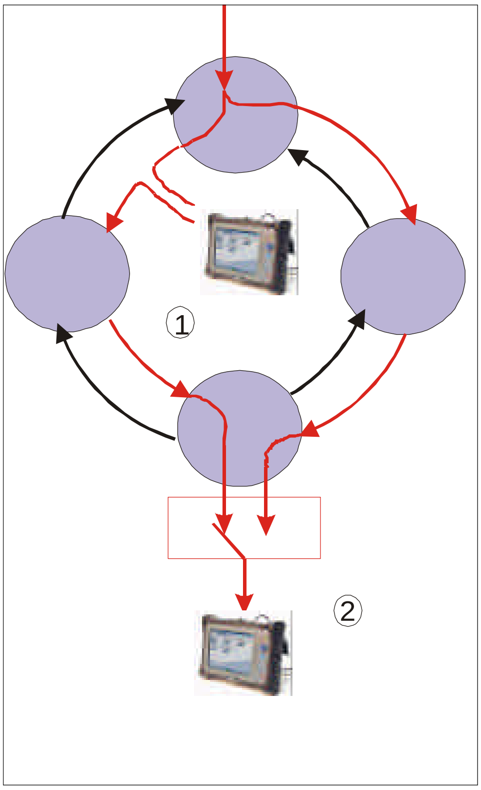
Unit 1 is optional. SF condition could also be simulated just by disconnecting the fiber. Nevertheless, the use of a CMA 5000 OTA allows to check that all the SD/SF criterias are taken into account by the network.

- the second for reading the results (shown as number 2).

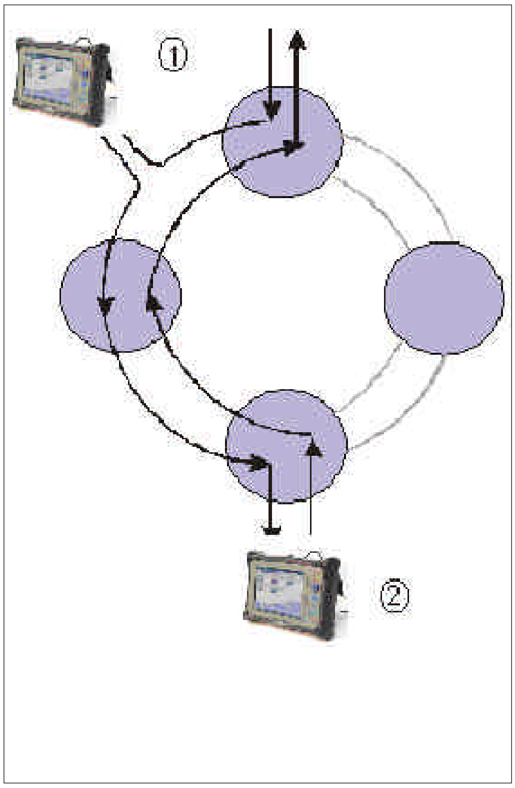
The place where the CMA 5000 OTA (used to generate the defaults) is connected depends on the network architecture.
The different cases are described hereafter:



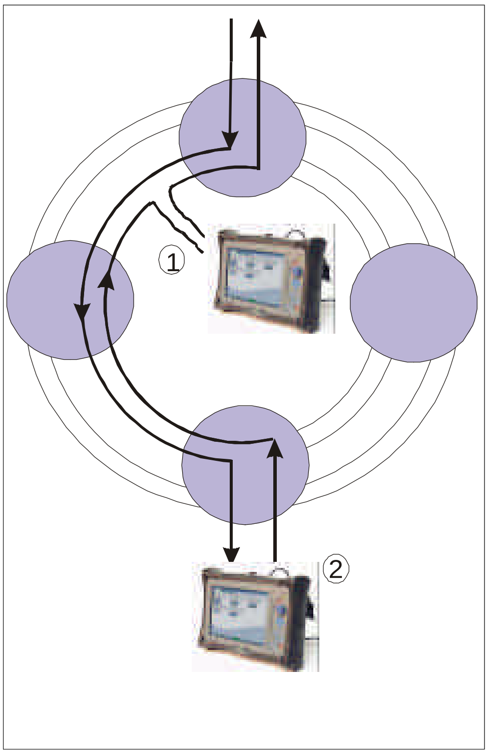
Linear architecture (1 + 1 or 1:N)



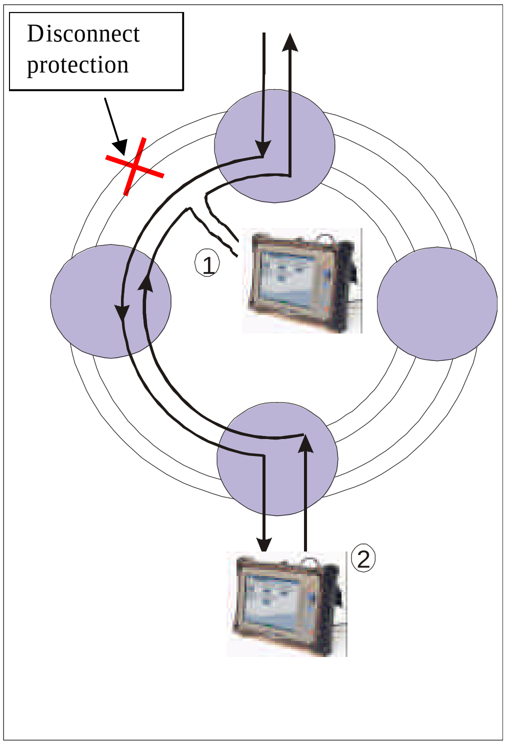
Ring architecture (SNCP)



Ring architecture (2F MS-SPRing)



Ring architecture (4F MS-SPRing : Span protection)



Ring architecture (4F MS-SPRing : Ring protection)

4.3 Configuring the OTA Application

Before starting the measurement, both CMA 5000 units must be configured.

CMA 5000 OTA N°1

This unit must be configured in Through Mode:

- Touch the “RX” tab to have access to the receive configuration window. Select the physical interface and the correct mapping structure.
- Touch the “TX” tab to have access to the transmit configuration window. Select the physical interface then touch the “Through-Mode” button.

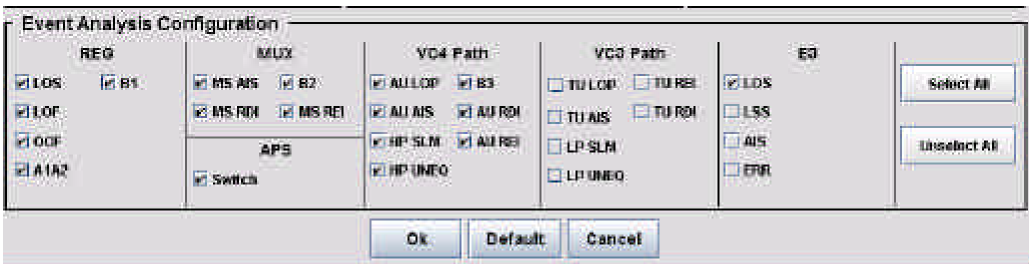
CMA 5000 OTA N°2

Only the reception needs to be configured.

- Select the APS measurement mode with the button “Select Measure”.
- Touch the “Rx” button to have access to the receive configuration window. Select the physical interface and the correct mapping structure.

In some case, it may be interesting to trigger the display of the “Event Analysis” window if certain alarms and errors occur.

- Touch the “General Setup” button and select your trigger events:



4.4 Generating Defaults in the Network in order to Initiate the Protection Process

The network must activate the protection process when a “default” occurs.
The recommendations define switch initiation criteria classified between “Signal Fail” and “Signal Degrade”.

With the CMA 5000 OTA N°1, you can generate calibrated defaults (alarms and errors) in order to simulate a Signal Failed or Signal Degrade condition:

- Touch the Stresses button
- Select Alarm/Error menu and the calibrated default you wish to generate:

In this example, we generate a MS-AIS (Signal Fail condition)

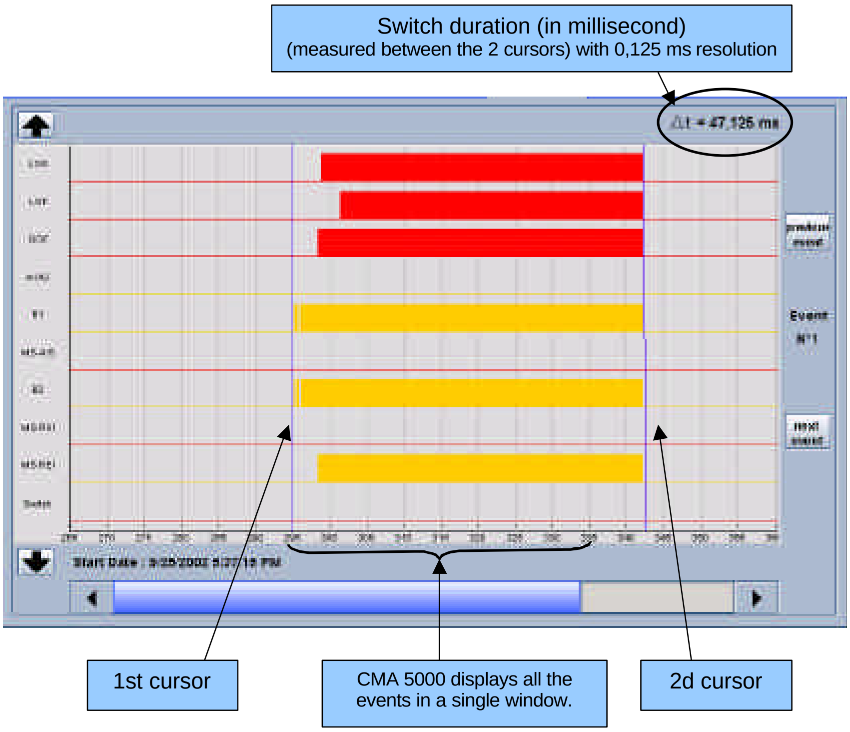
4.5 Reading the Results in the “Event Analysis” Window

Immediately after detecting the defaults, the network must start the protection process.
The duration window displays all the events that may appear during automatic protection switching in a single window with 125 µs resolution.
Two cursors are automatically positioned at the beginning and at the end of the defaults.
The time measured between the two cursors is displayed at the top of the window.

The results are readable on the CMA 5000 N°2:

• Touch the ‘Event Analysis’ tab

• Read the result:



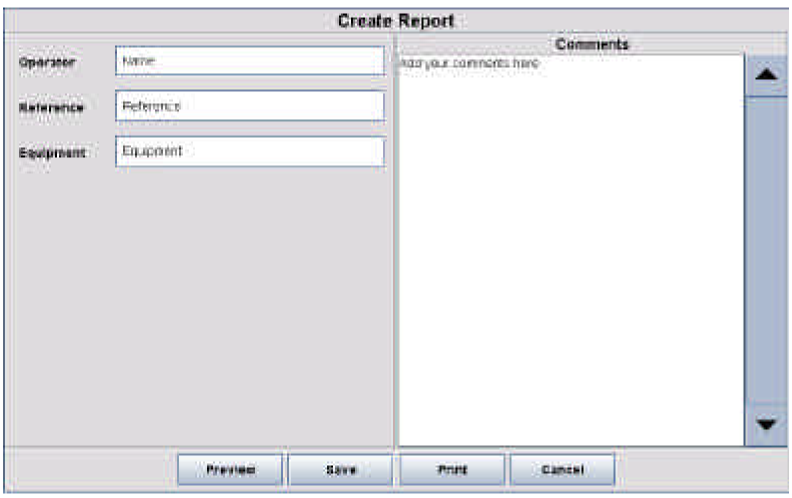
4.6 Saving the Results

After the measurement, you can create a professional test report.
This report is saved in a file and can be converted in a PDF format[1]. It is therefore possible to send by Email a professional test report to your customers or colleagues just 1 minute after the end of the measurement!

Creating and saving a test report with the CMA 5000 OTA N°2:

• Stop the measurement and touch the “Report” button

• Select “Create”. The next window will appear:



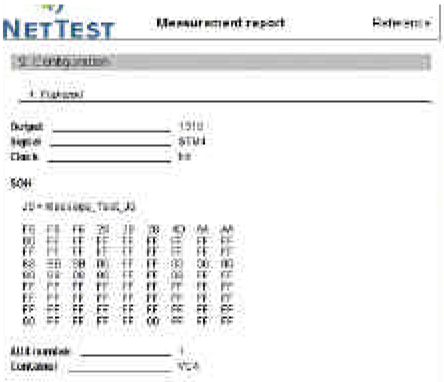
Notes:

[1] Adobe Acrobat Writer ™ required

• Enter your comments

• Touch “Preview” button. The OTA Application will display a report preview (see below)

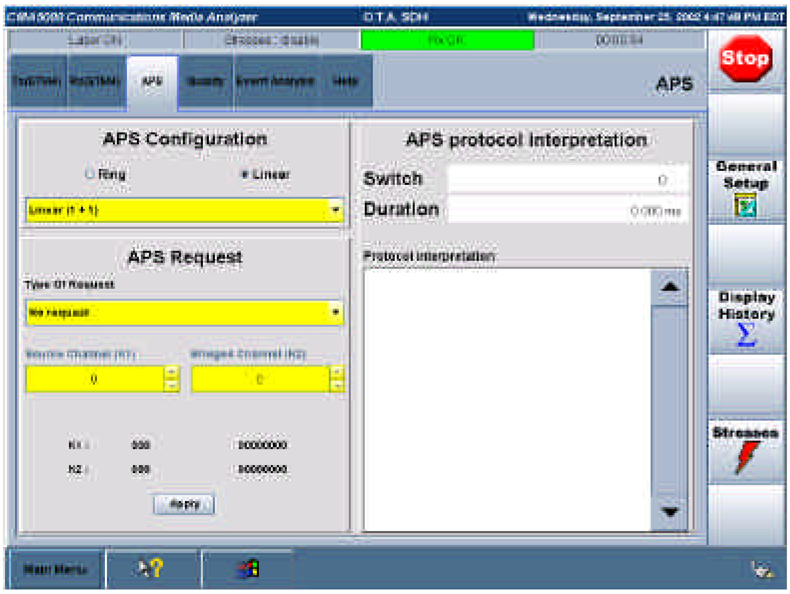
• To save the report, close the preview and then touch the “Save” button



5.0 Conclusion

The “Event Analysis” window of CMA 5000 OTA is a very powerful tool for people working on APS measurement. The results displayed in graphs (with 125 µs resolution) are easy to interpret.

The other aspect of the APS process is the protocol mechanism. The CMA 5000 OTA also provides a very useful window to manage this aspect. There is a special measurement mode called “APS” (Touch the button “Select Measure” and select “APS”). You will have access to the following window:



In this single window, you have access to all the information concerning APS measurement:

- APS architectures
- APS protocol requests generation
- APS switch time
- APS protocol interpretation

APS measurements have never been so easy!

NetTest A/S
Kirkebjerg Allé 90
DK-2605 Brøndby
Denmark
Tel: +45 72 11 23 00
Fax: +45 72 11 22 77
E-mail: nordic@nettest.com

NetTest Sales Offices

Australia	+61 3 9890 6677	Italy	+39 02 95 12 621
Brazil	+55 11 5505 6688	Mexico	+52 5557 8249
Canada	+1 905 479 8090	Singapore	+65 6220 9575
China	+86 10 6467 9888	Spain	+34 91 372 92 27
Denmark	+45 72 11 23 00	Sweden	+46 8 555 410 65
France	+33 1 61 34 34 61	UK	+44 (0)1883 349 110
Germany	+49 89 99 89 01 0	USA	+1 315 266 5000

NetTest, the pioneer in multi-layer network testing, is a global provider of test and measurement systems, instruments and components for all types of networks and all stages of network development and operation. Our solutions offer leaders in optical, wireless and fixed networking vital insights into network performance, enabling informed business decisions that drive profitability.