User Guide

Tempo Ethernet/Sync Installation Tool

Bottom traffic class		6.1 s
Step duration	4.000 ns	2.000 s

Color	IR (Mbit/s)	FLR	FTD (ms)	FDV (ms)
Green	7.698	1.920E-04	0.051	0.001
Yellow	3.012	0.000E-00	0.040	0.023
TOTAL	10.710	1.920E-04	0.141	0.001

Table Of Contents

Chapter 1: Introduction 1

Important Notice 2

Safety 3

WEEE Notice 3

The Tester 3

Test Connector Panel 4

Platform Connector Panel 6

The Graphical User Interface 7

The Home Panel 7

The Menu Structure 10

The Summary and LEDs Tabs 11

Recently Used Panel and Menu Tree 12

Predefined Tests 13

Running Tests 14

Upgrading the Unit 15

Chapter 2: Connection to the Network 17

Setting the Operation Mode 17

Connecting the Tester to the Network 20

Configuring the Connector 21

Using the SFP / SFP+ Ports 22

Configuring Port A and Port B Auto-negotiation Parameters 24

Entering the Port Local Settings 27

Using Pluggable Hardware Modules (PHMs) 30

Using the Traffic Reflector 30

Testing with an External Clock Reference 32

Using PPS / ToD, IRIG-B and Frequency References 39

Configuring the Built in GNSS Receiver 43

Using the Holdover Mode 47

Using the Clock Reference Output 50

Chapter 3: Cable Tests 57

Electrical Test 57

Basic Principles of Ethernet Cable Wiring 57
Connecting the Tester 59
Running the Test 60

Measuring Optical Power 64

Measuring PoE / PoE+ Electrical Parameters 64

Chapter 4: Traffic Generation 69

Generation of Ethernet Traffic 69
Physical Layer Settings 70
Frame Settings 70
Configuring the Bandwith Profile 77
Choosing the Test Payload for Ethernet 81

Generation of IPv4 Traffic 84
Configuring the Physical and MAC Layers 85
Configuring MPLS 86
Configuring the Port Local Network Profile 89
Configuring the IPv4 Datagram 90
Setting the Bandwidth Profile 94
Choosing the Test Payload for IPv4 94

Event Insertion 94

Chapter 5: Basic Frame Analysis 99

Global Counts and Statistics 100
Frame Counts 100
Error Counts 102
Network Counts 103
Bandwidth Statistics 105
Frame Size Distribution 107
MPLS Statistics 107

Using the Network Search Capability 108

The LEDs Panel 109

The Event Logger 113
Configuring the Event Logger 114
Displaying Logs 115
Exporting Logs 117

BER Testing 118

Framed BER Tests 118
Physical Layer BER Tests 120

Service Disruption Time 125

Chapter 6: Multi-Stream Analysis 127

Enabling and Disabling Filters 127

Configuring Filters 129
MAC Selection 130
C-VLAN and S-VLAN Selection 132
MPLS Selection 133
IPv4 Selection 135
IPv6 Selection 138
UDP Selection 140
TCP Selection 141
Protocol Selection 142
Fixed Offset Selection 144

Per-Stream Counts and Statistics 145
Bandwidth Statistics 146
SLA Statistics 147

Traffic Capture 150
Configuring the Capture 151
Controlling the Capture 152
Protocol Analysis 153
Capture Management through the Web Interface 154
Using Export Filters 156

Chapter 7: Automatic Performance Tests 159

Performance Assessment with the RFC 2544 Test 160
Throughput 161
Latency 163
Frame Loss 164
Back-to-Back Frames 165
System Recovery 166
Configuration Pass / Fail Thresholds 167
Getting Test Results 168
Generation of RFC 2544 Result Reports 172

Performance Assessment with the eSAM Test 175
Bandwidth Profiles for Ethernet Services 177
Test Configuration 181
CIR Configuration Test 187

EIR Configuration Test 188
Policing Configuration Test 188
Performance Test 190
Generation of eSAM Result Reports 191

Performance Assessment with the RFC 6349 194
Configuring the RFC 6349 Test 197
Setting the Performance Objectives 201
Retrieving the Results 202

Configuring the Test Method 206

Using the Responder Function 210

Chapter 8: Ping and Traceroute Tools 213

Ping 213
Internet Control Message Protocol 213
Test Configuration 214
Result verification 216

Traceroute 218
Test Configuration 218
Result verification 220

Chapter 9: PTP and NTP Analysis 223

Ethernet Synchronization with PTP and NTP 223
NTP Synchronization 224
PTP Protocol Details 224
PTP Synchronization Mechanism 225
PTP Protocol Encapsulation 226
Unicast Addressing Mode 226

IEEE 1588 Grandmaster and Slave Emulation 227
Configuration of the PTP Master and Slave 229
Protocol State 240
Message Statistics 245
Delay Statistics 247
Clock Status 252
Unicast Negotiation Results 254

The Pseudo-slave Emulation Mode 255
TE Test 256
Wander (MTIE / TDEV) Test 257
Floor Delay Population Test 262

PTP Passive Monitoring 266

NTP Server and Client Emulation 268
Protocol State 276
Message Statistics 279
Delay Statistics 281
NTP Pseudo-client Mode 283
TE Test 284

Chapter 10: Synchronous Ethernet Analysis 287
Introduction to Synchronous Ethernet 287
Ethernet Synchronization Messaging Channel 289
Synchronous Ethernet for the 1000BASE-T Interface 289
Frequency Measurement 292
MTIE / TDEV Analysis 292
Frequency Offset Generation 294
Wander Generation 295
Operation in IP Through Mode 296
ESMC Generation and Analysis 297

Chapter 11: GOOSE and SV Analysis 301
IEEE 61850 Performance Requirements 303
MMS, GOOSE, SV 304
GOOSE and SV Protocol Timing Analysis 308
GOOSE and SV Test Configuration 310
Running the GOOSE / SV Test 311

Chapter 12: Test Management 313
Generating Reports 313
Taking Screenshots 315
File Management 315
Saving Configurations 315
Renaming Files 316
Deleting Files 316
Exporting Files to External Devices 317
Importing Configurations 317
Verifying the Current Disk Usage 318
Configuring What to Do When the Disk is Full 318

Using the Embedded Web Server 318
Programming Tests 319
Using the System Menu 321
Using the Network 323
Installing Software Options 329
Upgrading the Power Management 330
Using NTP and GPS/NMEA for System Clock Synchronization 331
Using the Remote Control 333

Appendix A: Technical Specification 335
General 335
Operation Modes 335
Clock 336
Rubidium Reference 336
Built in GNSS 336
GNSS Compact Antenna 336
Clock Reference Inputs 337
Clock Reference Outputs 337
Ethernet PHY 337
Auto-Negotiation 337
Synchronous Ethernet 338
Power over Ethernet 338
Ethernet MAC 338
MPLS 339
IPv4 339
Generic / /UDP Traffic Generator 340
Bandwidth Profiles 340
Test Patterns and Payloads 340
Filter 340
Ethernet Selection 341
MPLS Selection 341
IPv4 Selection 341
IPv6 Selection 341
UDP / TCP Selection 341
Protocol Selection 342
PTP / IEEE 1588 342
NTP 342
PHY Results 343

Cable Tests 343
SFP 343
Auto-Negotiation 343
Synchronous Ethernet 343
Frame Analysis 343
Ethernet Statistics 343
MPLS Statistics 344
IP Statistics 344
Bandwidth Statistics 344
SLA Statistics 344
Service Disruption Time 344
BER 345
Network Exploration 345
PTP / IEEE 1588 Statistics 345
NTP Statistics 346
Automatic Tests 346
IETF RFC 2544 Test 346
ITU-T Y.1564 Test 346
IETF RFC 6349 Test 347
Port Loopback 347
ICMP Processor 347
Protocol Processor 348
Protocol Analysis 348
Platform 349
Power Specifications 349
User Interface 349
Results 349
Operational Ranges 349

Appendix B: Common Issues and Solutions 351

Chapter 1 Introduction

The Calnex Tempo is a dual port hand-held Ethernet traffic generator and analyser and is conceived to rate conformance and performance of native Ethernet networks or Ethernet services like Ethernet Private Lines (EPLs) or Ethernet Private LANs (EPLANs).

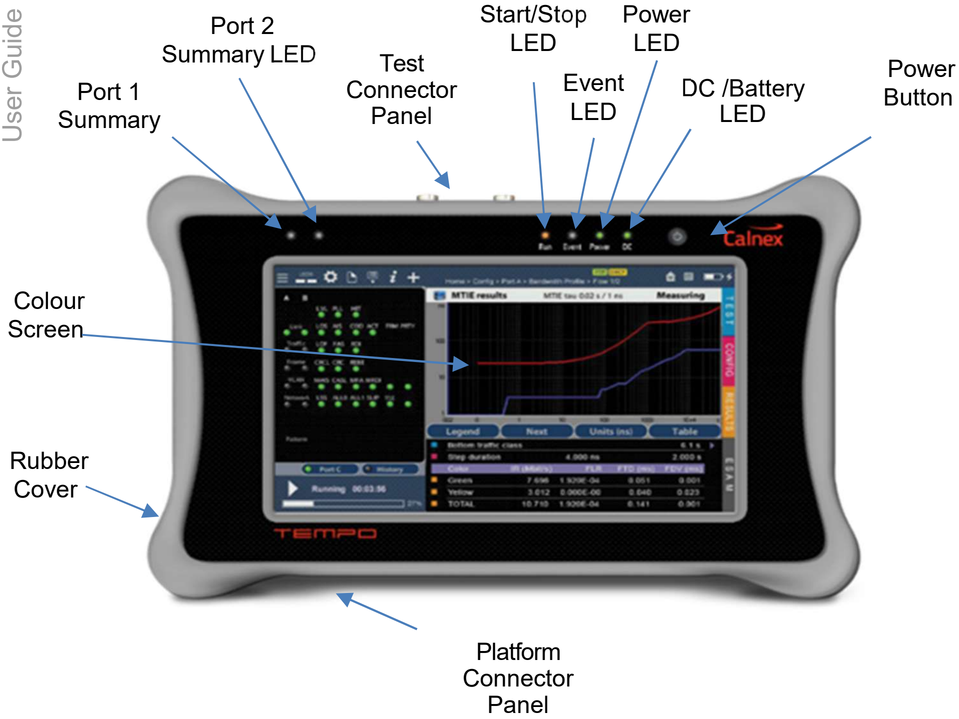


Figure 1.1: Tempo front view. The tester presents results by means a colour capacitive touch screen and the LEDs.

Tempo operates at bit rates up to 10 Gb/s. It comes with optional synchronization testing capabilities, advanced traffic capture and analysis tools and TDM monitoring and generation features. For this reason, Tempo is suitable for testing in environments where packet switching has not totally replaced legacy circuit switching technology, like in some cellular networks or electrical substations.

The test unit has an external DC input but it also has internal batteries. This makes this tester suitable both for laboratory applications and field applications which require versatile and reliable operation.

Within your Tempo test kit you will find the following items:

- One Tempo test unit.
- One AC/DC adapter with a power cord specific for your country.
- One Carrying bag.
- One Cat. 5e cable with RJ-45 connectors certified for operation at 1 Gb/s rates.
- Any additional cables, interfaces and modules ordered
- One coaxial cable with BNC male connectors.
- One USB memory stick with user documentation.

Check with your distributor the availability of other optional items for your Tempo unit.

1.1. Important Notice

Operation, manipulation and disposal warnings for your Tempo unit is listed below.

1.1.1. Safety

The Calnex Tempo test unit contains built-in batteries, improper use of which may result in explosion. Do not heat, open, puncture, mutilate, or dispose of the product in fire. Do not leave the device in direct sunlight for an extended period of time, which could cause melting or battery damage. Batteries must be replaced by Calnex authorized staff only. Use only the AC power adapter supplied by Calnex.

The equipment includes an active cooling mechanism. Do not block the air flow inputs and outputs during operation. Any use of this equipment other than the specified by the manufacturer may compromise the product electrical or mechanical safety.

The unit does not require any special maintenance. Use a soft cotton or microfibre cloth to keep your unit clean. A dry cloth for cleaning should be normally used. Using an aqueous product for cleaning is also allowable but it must be avoided putting liquid directly onto the equipment.

1.1.2. WEEE Notice

This product must not be disposed of or dumped with other waste. You are liable to dispose of all your electronic or electrical waste equipment by relocating over to the specified collection point for recycling of such hazardous waste. For more information about electronic and electrical waste equipment disposal, recovery, and collection points, please contact your local city centre, waste disposal service, or manufacturer of the equipment.

1.2. The Tester

Interaction with Tempo is based on a high resolution capacitive colour touch screen, and different kinds of status LEDs There are six LEDs (Run, Event, Power, DC, Port A summary, Port B summary). Their description is given below:

- *Run*: This is a LED that shows the current test status. The green colour is used to display a test running status. Off, means that there is no test running. Orange is displayed in the period of time between the action from the user to start / stop a test and the actual test start / stop.
- *Event*: A green Event LED is displayed when the equipment is generating some kind of impairment configured through the event insertion menu. The LED stays in off status when no event is being inserted
- *Power*: Displays the current tester on / off status. The green colour is displayed under normal operation conditions. Orange and red are shown to indicate a low battery load.
- *DC*: This led is lit when the DC input is connected. Orange indicates a *charging batteries* status and green means that the internal batteries are ready.
- *Port 1 / Port 2 Summary*: These LEDs provide a permanent indication of the current input signal (or signals) status. The LEDs summarize the Port A and Port B information given by the event LEDs. Or depending on the operation mode they may also summarize results from test Port C. If any event LEDs for a test port is in 'red' status, the port summary led will be set to 'red'. If any event LED is 'orange' but there is no 'red' event, the summary led will be set to 'orange. The 'green' col- our is used when no events are found in the input signal. Finally, the LED is switched off when the port is disabled.

The information supplied by the LEDs is also available in the screen so that there is not information loss when users access to the unit remotely (See section 12.6).

Users willing to use a mouse and keyboard are allowed to do so by connecting these devices to the USB port placed in the platform connector panel (See section 1.2.2).

There is a single button in Tempo that is used to switch the unit on and off. If the tester is in off status, push to switch it on. If the tester is on, use this key to switch it off (long push). The on / off button is also used for some other purposes like the test unit software upgrade (See section 1.5).

1.2.1. Test Connector Panel

Tempo is connected to the DUT / SUT through the test connector panel. Ports and elements included in this panel are described in the following list:

- *RJ-45 Port A*. This is the primary 10/100/1000BASE-T port for Ethernet transmit and receive.
- *RJ-45 Port B*. This is the secondary 10/100/1000BASE-T port for Ethernet transmit and receive. This port is identical to the RJ-45 Port A in appearance but it provides only a subset of the features available for Port A. Port B supports monitor

and loopback operation but it does not include traffic generation.

- *SFP Port A*: This port is used to connect the tester to the network through an optical interface with the help of an SFP module.
- *SFP Port B*: This port is used to connect the tester to the network through an optical interface with the help of an SFP module.
- *SFP+ Port A*: This port can be used also with SFP+ modules compatible with 10 Gb/s transmission.
- *SFP+ Port B*: It can be used also with SFP+ modules compatible with 10 Gb/s transmission.

- *BNC Port C RX*: Unbalanced 75 Ω input. This input is used to analyse clock (1544 kHz, 2048 kHz, 10 MHz) and TDM (E1 and T1) signals. It is used as a clock reference input port as well.
- *BNC Port C TX*: Unbalanced 75 Ω output. This output is used to generate TDM signals (E1 and T1). It is used as a clock output as well.

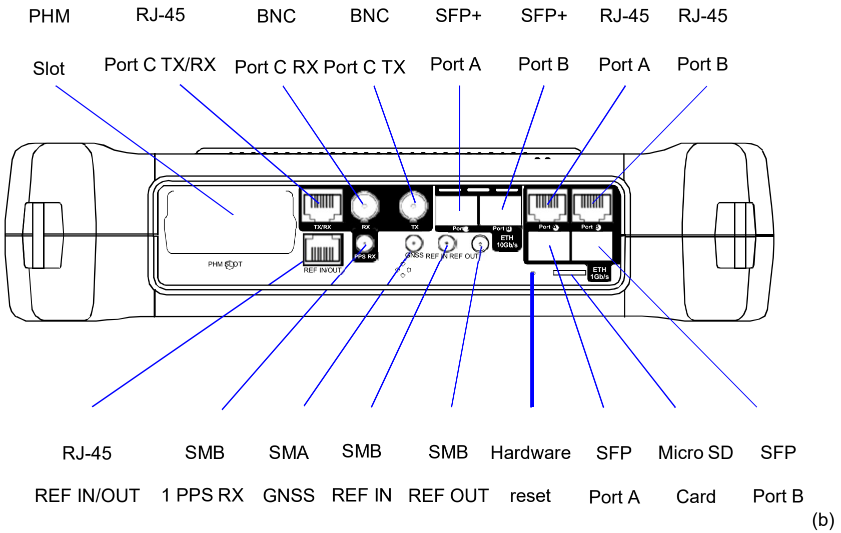


Figure 1.2: Test connector panel. Connection to the DUT / SUT is done in this panel

- *RJ-45 Port C TX/RX*: Balanced 120 Ω input / output. This interface is used to analyse clock signals (1544 kHz, 2048 kHz, 5 MHz 10 MHz, 1 PPS, 1 PP2S) and generate and analyse TDM (E1 and T1) signals. This interface is used as a clock input / output as well.

- *SMA GNSS*: This is a SMA connector that can be used to attach a GNSS antenna. The purpose of the GNSS input is to provide a reliable and accurate synchronization source for the test unit (See section 2.6.2).
- *SMB Port C PPS RX*: 1 PPS 1 PP2S test input. This is the port to be used for analysis of unbalanced 50 Ω 1 PPS signals formatted as specified in ITU-T G.8271.
- *SMB REF IN*: 1 PPS reference input. This port could be used as a 1 PPS clock reference input used in some latency and synchronization tests. This is an unbalanced 50 Ω interface that follows standard ITU-T G.8271.
- *SMB REF OUT*: 1 PPS reference output. This port could be used as a 1 PPS clock reference output. The output is synchronized with the local oscillator. This is an unbalanced 50 Ω interface that follows standard ITU-T G.8271.
- *RJ 45 REF IN/OUT:* Reference input / output. It generates or accepts balanced 1544 kHz, 2048 kHz, E1, T1, 5 MHz, 10 MHz, 1PPS and 1PP2S clock references.
- *PHM Slot:* Enables connection of a *Pluggable Hardware Module* (PHM) to the test unit. The currently available PHMs include the datacom module, the dual port IEEE C37.94 module, the G.703 / E0 module and the voice frequency module.
- *Micro SD Card*: Slot for micro SD Cards. These cards can be used as external storage devices.
- *Hardware reset*: Resets the hardware to recover the unit from most malfunctioning situations.

1.2.2. Platform Connector Panel

There is a connector panel specifically devoted to the platform ports. This panel includes capabilities like remote control and external device connection. A more detailed description is given below:

- *Power connector*: The input must be 12 V DC, 4 A. A suitable external AC / DC adapter for your country is provided with the tester.
- *RJ-45 printer or console*. Console connector. Not currently used.
- *USB Master*: Use a USB cable with a Master type connector (Type A, *Host*) for this port. Currently this port is used for software upgrades and connection of external storage devices.
- *RJ-45 platform LAN connector*: This is a general purpose Fast Ethernet connector (10/100BASE-T). It is used for remote management of the test unit or to access to the configuration, report and trace files through a web interface.

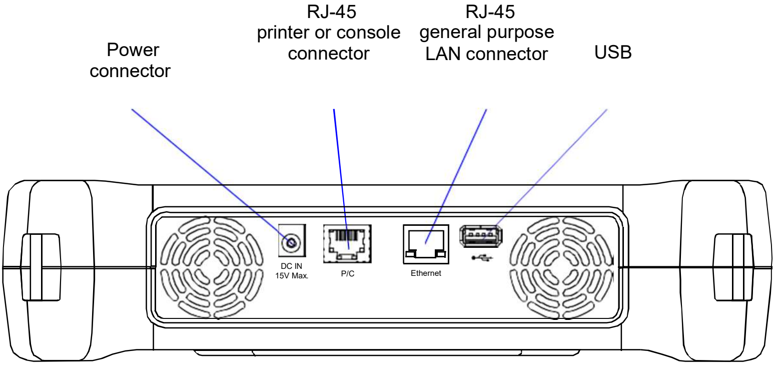

Power connector
RJ-45 printer or console connector
RJ-45 general purpose LAN connector
USB
DC IN 15V Max.
P/C
Ethernet

Figure 1.3: Platform connector panel. This panel includes connectivity to USB devices, Ethernet networks and power source.

1.3. The Graphical User Interface

The Tempo graphical user interface is based in a 800 x 480 colour touch screen that can be used to browse the different panels, configure the unit and start / stop tests.

1.3.1. The Home Panel

To display the Home panel, users must press the *Home* button (square icon on the top right corner of the screen). The *Home* panel contains two sub-panels with miscellaneous information. The main panel enables the user to configure a test, modify the port settings or check results from the current or a past test, the auxiliary panel contains miscellaneous information. There are three buttons in the main panel to enable the user to access to these resources:

- *TEST*: Contains configuration items related with general test configuration like test scheduling, test setup, performance objectives settings, event insertion, and event logging. Configuration of some special tests like the RFC 2544 or the eSAM or the Ping / Traceroute is also done from this menu. Finally, setting of some special operation modes like the PTP endpoint emulation is available in this menu as well (only in units with the correct PTP or Synchronous Ethernet licenses installed)
- *CONFIG*: Provides access to the global operation mode and configures test ports and other resources such as reference clock inputs and outputs, secondary interfaces, etc. The setup menu can be used to configure the test ports A and B.In

units with the correct software options installed, it may also include menus to configure the E1 / T1 and other test interfaces.

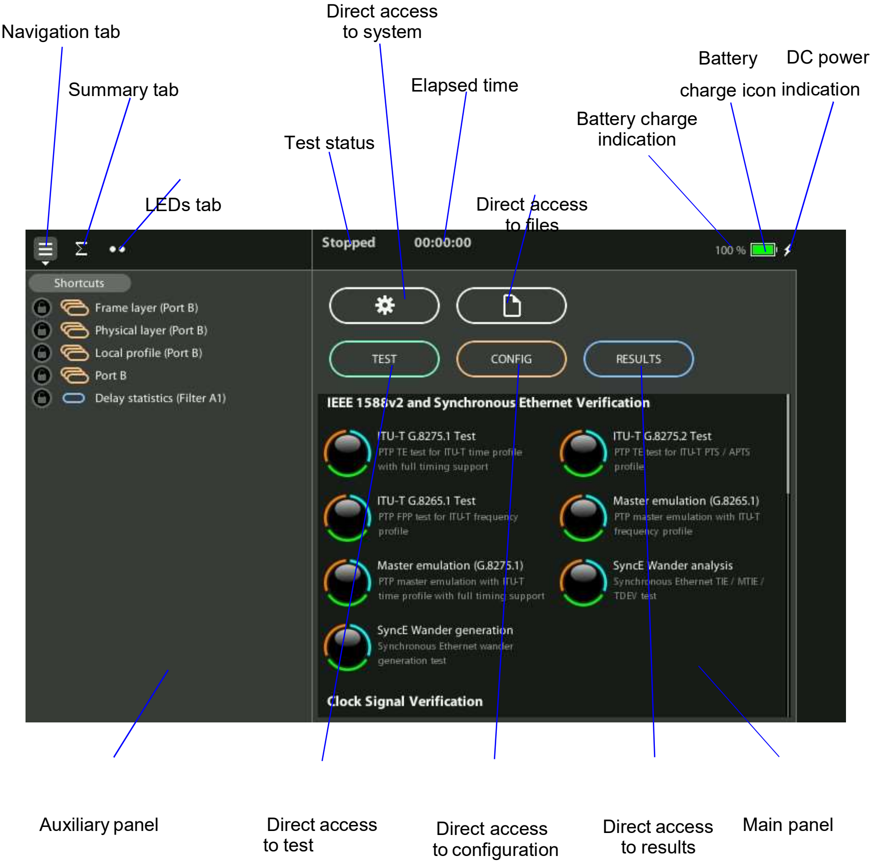

Navigation tab
Direct access to system
Summary tab
Elapsed time
Battery charge icon
DC power indication
Battery charge indication
Test status
LEDs tab
Direct access to files
Stopped
00:00:00
100 %
Shortcuts
Frame layer (Port B)
Physical layer (Port B)
Local profile (Port B)
Port B
Delay statistics (Filter A1)
TEST
CONFIG
RESULTS
IEEE 1588v2 and Synchronous Ethernet Verification
ITU-T G.8275.1 Test
PTP TE test for ITU-T time profile with full timing support
ITU-T G.8275.2 Test
PTP TE test for ITU-T PTS / APTS profile
ITU-T G.8265.1 Test
PTP FPP test for ITU-T frequency profile
Master emulation (G.8265.1)
PTP master emulation with ITU-T frequency profile
Master emulation (G.8275.1)
PTP master emulation with ITU-T time profile with full timing support
SyncE Wander analysis
Synchronous Ethernet TIE / MTIE / TDEV test
SyncE Wander generation
Synchronous Ethernet wander generation test
Clock Signal Verification
Auxiliary panel
Direct access to test
Direct access to configuration
Direct access to results
Main panel

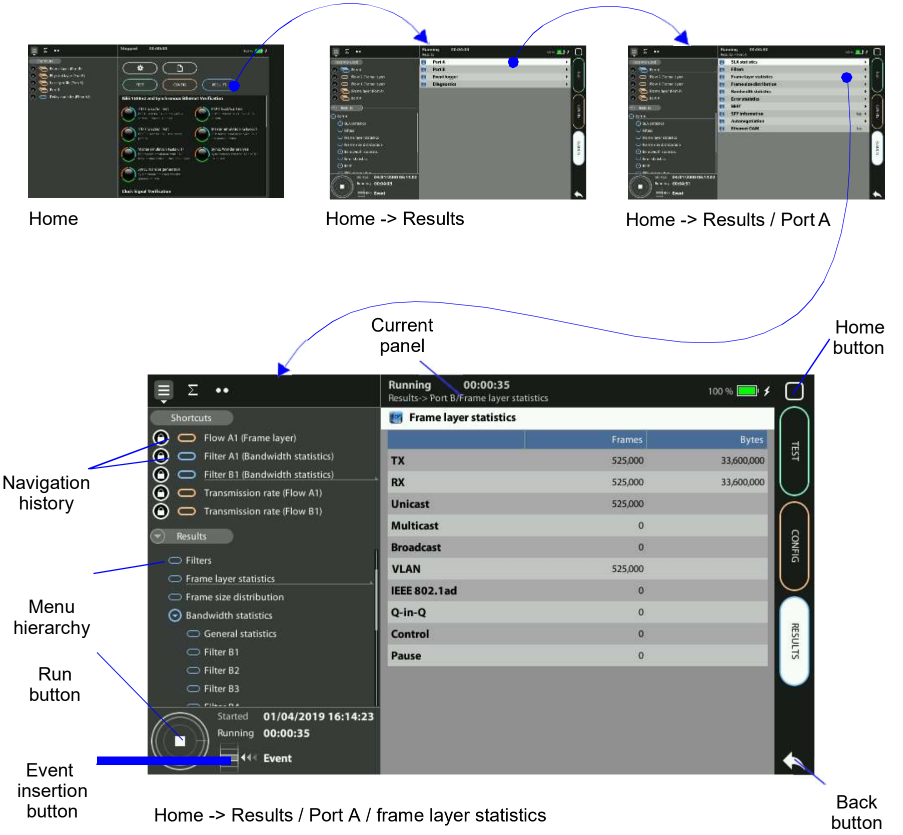
Figure 1.4: Tempo home panel.

- *RESULTS*: This item enables the user to browse test results. Most of them are not available if a measurement has not been previously started but there are some exceptions to this rule. The Results panel also contains access to the Event logger browser, that enables the user to display graphically miscellaneous events and performance metrics.

There are two additional buttons in the main panel not directly related with testing tasks but with test unit management. These are the *File* and *System* buttons and they have the following purpose:

- *File*: File management menus. Includes configuration, report and trace file management. Files can be deleted, copied, exported or imported.

- *System*: Provides platform management tools. For example language selection, screensaver configuration and others.



Frame layer statistics

	Frames	Bytes
TX	525,000	33,600,000
RX	525,000	33,600,000
Unicast	525,000	
Multicast	0	
Broadcast	0	
VLAN	525,000	
IEEE 802.1ad	0	
Q-in-Q	0	
Control	0	
Pause	0	

Figure 1.5: Access to a results table from the home panel in three different steps. In this case the test results are represented as a table, including a header (frames, bytes), a results list (TX, RX ,...) and different counters.

The main panel may also contain shortcuts to predefined tests users are allowed to load depending on what they need to do. The number and type of these shortcuts depend on the license included in the test unit.

On the left side of the main panel there is an auxiliary area with three tabs:

- *Navigation tab*: Includes a *Recently Used* area to enable the customer to go to specific panels without the need to go through any intermediate panel and a menu tree to display the panel hierarchy corresponding to the *TEST*, *CONFIG* and *RESULTS* menus (or *File* and *System* menus).

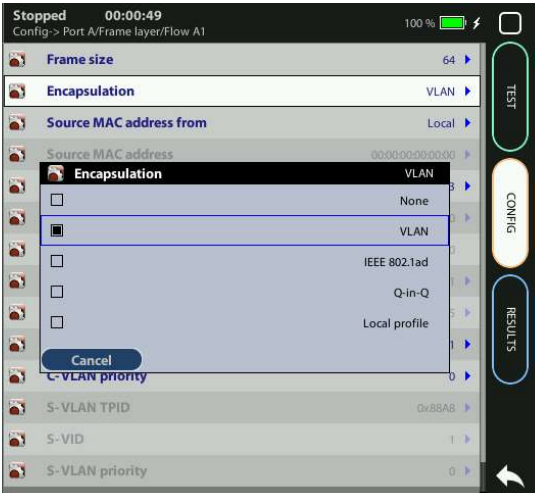
- *Summary tab*: Has information about protocol stacks, traffic flows, filters, frame structures and some other details about the test unit configuration. It may also include relevant results in some configurations.
- *LEDs tab*: Displays visual information about status. Most LEDs are referred to test signal status but some others may be related clock references or other subsystems. The LEDs may display real time information but the can be also configured in *History* mode to store details about past events.

On the top side of the home panel there is a header zone which contains information about the current tester status (date, time, tests running, event insertion active) and an identifier for the currently displayed panel.

The *Navigation*, *Summary* and *LEDs* tabs, together with the header zone are replicated in all other *TEST*, *CONFIG* and *RESULTS* screens. The difference is that in screens other than the *Home* panel there is also a test control area to enable the user to start / stop tests or to add events to the outgoing signal.

1.3.2. The Menu Structure

Most of the graphical user interface panels are menus containing a variable number of items. Menus and sub-menus are organized in a tree. The tree root is the *Home* panel and the leaves are configuration or result panels. Results are usually presented in a list or a table. If all results cannot be simultaneously displayed, then the user is allowed to scroll up and down to browse the list. An scroll bar shows the current position in the menu if there is no room to display all items at the same time.



Stopped 00:00:49
Config-> Port A/Frame layer/Flow A1

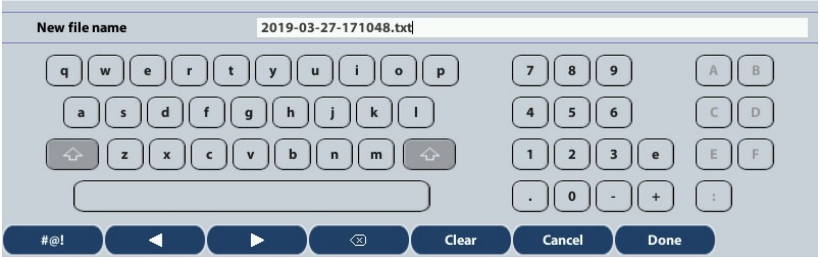
Frame size 64
Encapsulation VLAN
Source MAC address from Local
Source MAC address 00:00:00:00:00:00

Encapsulation VLAN
□ None
■ VLAN
□ IEEE 802.1ad
□ Q-in-Q
□ Local profile

C-VLAN priority 0
S-VLAN TPID 0x88A8
S-VID 1
S-VLAN priority 0

Figure 1.6: Tempo selection panel to enable users to choose between different Ethernet encapsulations

Configuration and result panels are conceptually different to menus even if both kinds of items could be displayed under the same higher level menu. For this reason they are displayed in a different way. While menus are described with black characters configuration and result panels are displayed in blue characters. The second difference is that only menus are displayed in the menu hierarchy (*Navigation* tab).



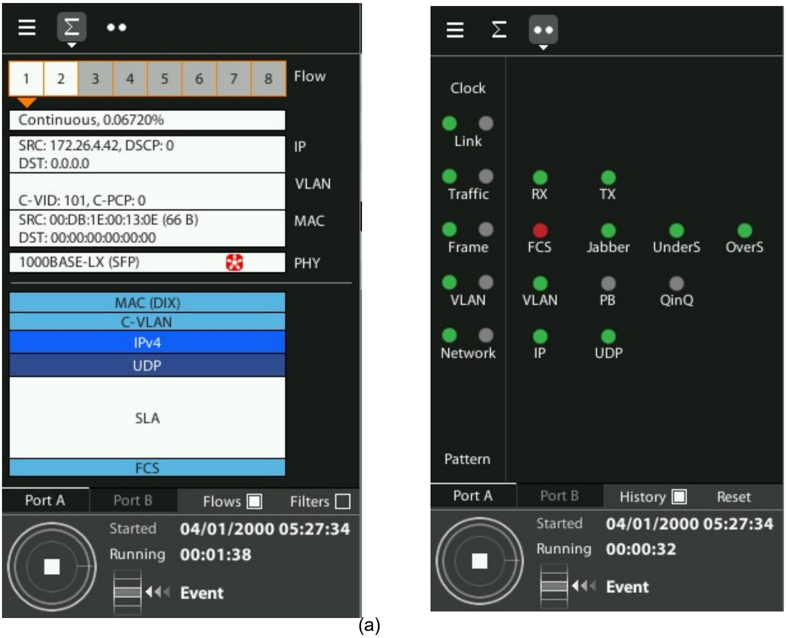
New file name 2019-03-27-171048.txt

Figure 1.7: Data input keyboard. The keyboard is used to enter alphanumeric, numeric and hexadecimal characters.

Configuration panels are usually selection lists. Sometimes you can select only one simultaneous item in the list and sometimes selection of several items at the same time is possible. Keyboards are available if selection through lists is not possible. There is one keyboard for numeric settings and one for alphanumeric settings. These keyboards are also used to enter data types with a well defined formatting such as IP or MAC addresses.

1.3.3. The Summary and LEDs Tabs

The test signal status can be checked from the LEDs tab on the top left corner of the screen. The Softleds from the LEDs panel are always active, even when there is no test running. The LEDs may display real time information but they can be also configured in *History* mode to store details about past events. They are organized in rows and columns each row usually includes LEDs with a related meaning. Typically (but not always), events displayed in the same row correspond with the same protocol layer. For each row, there is a summary LED, which aggregates the result for all items in the same row. The results from the same summary column are also aggregated in a single hardware port summary LEDs.



Continuous, 0.06720%

SRC: 172.26.4.42, DSCP: 0
DST: 0.0.0.0

C-VID: 101, C-PCP: 0

SRC: 00:DB:1E:00:13:0E (66 B)
DST: 00:00:00:00:00:00

1000BASE-LX (SFP)

Started 04/01/2000 05:27:34
Running 00:01:38

(a)

Started 04/01/2000 05:27:34
Running 00:00:32

(b)

Figure 1.8: Special panels: (a) Summary panel, (b) LEDs panel.

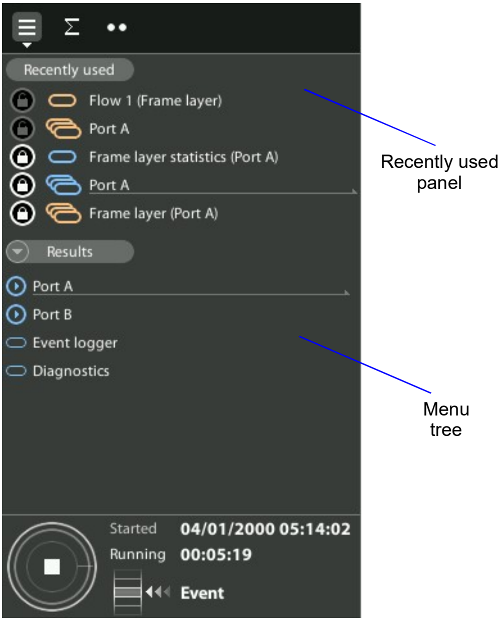
The *Summary* tab provides some details about the current configuration and results. There is not a fixed structure for this tab, which has its own layout depending on the currently selected operation mode.Typically, this panel has graphical information about traffic flows, protocol stack, filters, signal processing blocks, etc.

1.3.4. Recently Used Panel and Menu Tree

The *Summary* tab has two differentiated areas. The *Recently Used* area provides quick access to important screens, the *Menu tree* contains the *TEST*, *CONFIG* or *RESULTS* menu trees with a general view of the choices available to users.

- *Recently Used panel*: Each new screen visited by the user is listed in the *Recently Used* panel. New screens replace the older screens so that the oldest in the list is deleted when a newer one is visited. The *Recently Used* panel may contain up to five screens. To avoid any of the listed screens to be deleted from the list, users may lock them by pressing the *lock* button on the left of each screen. Locked screens can be unlocked by pressing the *lock* button a second time.

- *Menu Tree*: Contains the list of all sub-menus available in each of the *TEST*, *CONFIG* and *RESULTS* panel. Menus and sub-menus can be opened to display lower order sub-menus. Direct access to menus is possible by pressing the correct destination in the *Menu Tree*. Only menus are displayed in the tree. No configuration or result panels are shown in this area.



Started 04/01/2000 05:14:02

Running 00:05:19

Recently used panel

Menu tree

Figure 1.9: The Summary tab contains a Menu tree and the Recently Used panel.

1.3.5. Predefined Tests

Predefined tests are special shortcuts located in the *Home* panel that enable Tempo users to access to common test scenarios without having to configure the unit step by step. The predefined test shortcuts configure most test parameters and provides quick access to the (usually few) parameters still to be configured.
Specifically, the predefined test shortcuts do the following tasks:

- Displays a specific panel in the work-area that depends on the predefined test that has been loaded.
- A variable list of settings is configured in the unit such as operation modes, ports, interfaces and tests. The user interface, work area and all other complementary panels are upgraded in accordance with the new settings.

- Loads a list of shortcuts in the *bookmarks-list* that depends on each predefined test. The panel displayed on loading the predefined test is the first item in the bookmarks-list.

Predefined tests have been distributed in four categories: *IEEE 1588v2 and Synchronous Ethernet Verification*, *Clock Signal Verification*, *Ethernet / IP Verification*, *E1 / T1 Verification*. It follows a description of the tests included in each category:

- IEEE 1588v2 and Synchronous Ethernet Verification: *ITU-T G.8275.1 Test*, *ITU-T G.8275.2 Test*, *ITU-T G.8265.1 Test, Maser emulation, (G.8265.1)*, *Master emulation (G.8275.1)*, *SyncE Wander analysis*, *SyncE Wander generation*.
- Clock Signal Verification: *1PPS TE*, *1PPS to 1PPS TE*, *10 MHz TIE*.
- Ethernet / IP Verification: *RFC2544 (bridged, port A > B), RFC2544 (routed, port A > B)*, *eSAM (bridged, port A > B)*, *Traffic verification (bridged)*, *Traffic verification (routed)*, *Ping*, *Trace-route, TCP throughput (RFC6349).*
- E1 / T1 Verification: *E1 / T1 Pulse Mask*, *E1 / T1 BER*, *G.821*, *G.826*, *E1 / T1 Jitter*, *E1 /T1 Wander*, *E1 / T1 RTD*, *E1/T1 OWD*,

1.4. Running Tests

Most of the results provided by the test unit are not available until you start a test. This section provides a high level description of the procedure to follow to configure your unit, start a test and review the results.

1. Configure the tester to send / receive signals in the right operation mode and through the right ports using the resources from the *CONFIG* menu. Connect it to the network.
2. Configure the specific parameters such as pass / fail objectives, test method or any other setting required for your test using the *TEST* menu.
3. Program the test start time and duration with the help of the *Autostart / stop* menu (within *Test*) or start the test immediately by pressing the *run* button in the test control area.
   Note: Most of the configuration is blocked when there is an ongoing test.
4. Wait for the test to finish or press *run* to finish immediately.
5. Check the test results in the *Results* menu.
   Note: Most test results are upgraded in real time as the test progresses. That means that is not really necessary to wait for the test to finish to check current results.

It must be stressed that this is only a high level description of test configuration and execution using Tempo. For a detailed description of the configuration procedures for specific tests visit the corresponding sections in the User Guide.

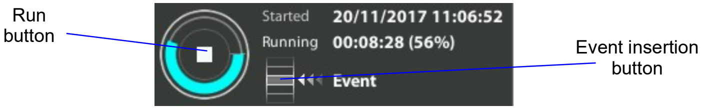


Figure 1.10: Tempo test control area with progress indication.

1.5. Upgrading the Unit

The test unit software can be upgraded with the help of a USB memory stick. Before proceeding with the upgrade, copy the Calnex software to the root directory in the memory stick. The file name of the upgrade package must not be modified. The USB must have a FAT32 file system.

Once the USB memory stick is ready. Follow this procedure to install the new software:

1. Switch the unit off.
2. Press the *Power* button and keep the button pressed until you see the *Power* LED to start blinking.
3. Release the *Power* button.
   You will hear a beep and the Calnex Software Installer will be loaded and executed. An informative panel will display the Tempo software version num- ber found in the storage device.
4. Press *Continue* to continue with the installation process or *Cancel* to finish.
5. Select *Install* or *Upgrade. Install* regenerates all the software in the unit even if it is up to date. Upgrade regenerates only the software that has changed since the last upgrade. Use *Install* if you need to recover the unit after operation failure due to corrupted software. Use *Upgrade* otherwise.You can also cancel the process at this point by pressing *Cancel*.
6. Confirm your previous selection by pressing *Continue* or cancel with *Cancel*.
7. Wait for the installation process to finish.
   Note: The full process may take a few minutes.
   Note: Do no disconnect the unit or remove the USB memory stick during installation.
8. Press *Continue* to close the Software Installer and finish the installation process. The unit will be automatically restarted. The new software will be loaded.

Chapter 2

Connection to the Network

The test unit is equipped with two identical 1 Gb/s RJ-45 ports, two 1 Gb/s SFP ports, and, in case of Tempo, two additional 10 Gb/s SFP+ ports. The RJ-45 ports are used for connection to Ethernet electrical interfaces. The SFP and SFP+ ports are normally used for optical connections. Each RJ-45 / SFP / SFP+ interface constitutes a single logical port. These ports are labelled as Port A and Port B.Tempo includes a third port (Port C) for TDM and clock signal generation and analysis and a PHM slot that can be used to attach custom modules for test applications not included in the Tempo mainframe. For more information about how to use PHMs read the *Tempo TDM Testing Guide*.

In a full featured unit Port A and Port B share the same generation and analysis capabilities. However, depending on the licensing options, Port B may not include advanced traffic generation. In units without the dual port generation capability, Port B can loop frames / packets toward their origin if configured to do so. It also responds to pings (ICMP echo request message) and other basic protocols like ARP.

Analysis capabilities of Port A and Port B are similar with some exceptions like the cable test, the PoE / PoE+ analysis or most synchronization tests.

This chapter describes how to connect the tester to the network and how to configure it to receive and send signals. The general, high level procedure to do that is:

1. Configure the Port A / Port B, including global and port specific operation modes and generation / analysis properties.
2. Connect the test cables to the network. Use the electrical or optical ports depending on the particular network properties.
3. Traffic generation does not start until you start a test with the run key. Most of the results are not available neither.

2.1. Setting the Operation Mode

As Ethernet interfaces, Port A and Port B are independent but they share the same global operation mode. That means that, for example, if you configure Port A to be an

IP endpoint port, then Port B will become an IP endpoint port as well. In any other sense, Port A and Port B are allowed to have a different configuration.

To configure the Tempo global operation mode follow these steps:

1. From the *Home* panel, go to *CONFIG*,
   The port configuration panel is displayed.
2. Select *Mode* to enter in the mode selection menu
3. Choose between: *Ethernet endpoint*, *IP endpoint*, *IP Through*, *Ethernet cable test*
   Note: Some other operation modes may be available depending on the hardware / software options available in your test unit.

Table 2.1: Global Ethernet Operation Modes

Mode	Description
Ethernet endpoint	If the tester is configured in *Ethernet endpoint* mode, then it emulates an Ethernet network terminating point. In this mode the generator sends a test signal made up of Ethernet frames to the DUT / SUT and the analyser receives new Ethernet frames from the DUT / SUT. The received signal may be the same test signal once it has been transmitted through the DUT / SUT. This mode is used for continuity / transparency testing, BER testing and performance (SLA, eSAM, RFC 2544) measurements in Ethernet interfaces. You can use this operation mode if you have IP over Ethernet but you don’t care about the network protocol used in the network.
IP endpoint	If the tester is configured in *IP endpoint* mode, then it emulates an IP network terminating point. In this mode the generator sends a test signal made up of IPv4 frames to the DUT / SUT and the analyser receives new IPv4 / IPv6 frames from the DUT / SUT. The Received signal may be the same test signal once it has been transmitted through the DUT / SUT. This mode is used for continuity / transparency testing, BER testing and performance (SLA, eSAM, RFC 2544, RFC 6349) measurements in IP / Ethernet interfaces.
IP through	The *IP Through* mode is suited for bidirectional intrusive monitoring. The signal from the Port A receiver is forwarded to the Port B transmitter. An equivalent operation is performed on the signal received on Port B. As it passes through the test unit, the test signal is analysed and statistics about it are collected and recorded.

Table 2.1: Global Ethernet Operation Modes

Mode	Description
Ethernet cable test	This is the correct mode to check the UTP / FTP / STP cable transmission parameters like the wire map, skew and MDI / MDIX port status. If there is any cable fault like an open or a short circuit, it is detected and an estimated distance to the fault is displayed. If this mode is enabled, port B is forced to a *Link* status and port A is set to an special *Cable test* status that is specifically used for cable tests.
L1 endpoint	This is a mode specifically conceived for physical layer BER tests. When the equipment is configured in this mode is unable to generate user-configurable frames but it can still generate and analyse the PCS codes required for BER testing at L1.

There is a port specific operation mode that is complementary to the global operation mode. Both the global and the port specific operation modes are combined to determine which tests and which capabilities are available at any moment.

Table 2.2: Port Modes

Mode	Description
TX / RX	Both transmission and reception are enabled in the port. The transmitter is connected to the internal test traffic generator. This is the port mode to be used most of the times for testing in endpoint mode.
Monitor	The port is configured in promiscuous monitoring mode and the port transmitter is disabled. All kinds of traffic generation are disabled in *Monitor* mode but the equipment can still reply to some ARP and ICMP requests for technical reasons. Use this mode if you want to get statistics about the network traffic, including traffic from remote test unit but you don’t want to disturb the network with any test traffic internally generated by the unit.
Loopback	The port receiver is connected to the transmitter so that part or all the received frames are sent towards the origin. This port mode is used guarantee the continuity of the test payload or pattern to in two-way tests.

Table 2.2: Port Modes

Mode	Description
Cable test	This is a mode specifically used for cable tests. It is used if the global operation mode is set to *Ethernet cable test*. The *Cable test* port mode disables transmission of Ethernet frames or IP packets. It also stops any layer 2 or layer 3 analysis. The *Cable test* port mode is available for port A only.
Link	This is a mode specifically used for cable tests. It is used if the global operation mode is set to *Ethernet cable test*. The *Link* test mode disables transmission of Ethernet frames or IP packets. It also stops any layer 2 or layer 3 analysis. The only function of the *Link* port mode is to supply link to enable *Port A* to measure the all cable parameters. The *Link* port mode is available for port B only.
Disabled	Both the port transmitter and receiver are disabled. Use this mode if you are not going to use the corresponding port and you want to extend the operation time with batteries to the maximum.

To configure the test unit port specific operation mode follow these steps:

1. From the *Home* panel, go to *CONFIG*,
   The port setup panel is displayed.
2. Select either *Port A or Port B* to enter in the port specific configuration menu.
3. Select *Port mode* to enter in the mode selection Menu
4. Choose between: *TX / RX*, *Monitor*, *Loopback, Cable test, Link* or *Disabled*.
   Note: Some other operation modes may be available depending on the global operation mode and the actual port you are configuring.

2.2. Connecting the Tester to the Network

The way you connect your tester to the network depends on the global operation mode. For example, if you set the tester to operate in *IP through* mode, you will be required to connect the equipment in “transparent” mode, with the traffic going through the unit from Port A to Port B and Port B to Port A.

The operation mode also depends largely of the type of DUT / SUT. If you are connecting the equipment to an IP router, probably it does not make sense to configure the equipment in *Ethernet endpoint* mode because the router will be unable to recognise and forward traffic without an IP payload. Note that the opposite is not true. You may want to send IP traffic trough an Ethernet network and for this reason, the *IP* *endpoint* mode is compatible with Ethernet network testing. Many users (carriers and service providers) are offering Ethernet services like Ethernet Private Lines (EPLs) or Ethernet Private LANs (EPLANs) and they prefer to avoid making any decision concerning IP addressing. They also prefer to avoid generation of any IP stack protocol (ICMP, ARP, DHCP, PPP) within their administrative domains. For these users, the *Ethernet Endpoint* mode is the most appropriate.

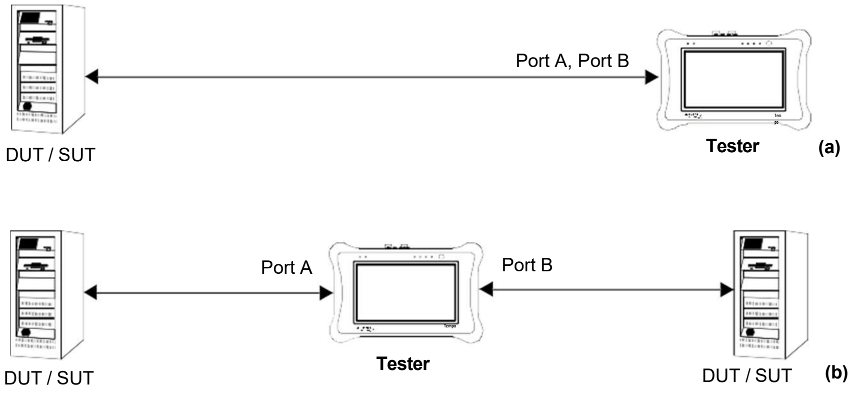


Figure 2.1: Basic connection setup for Tempo testers: (a) Ethernet and IP endpoint operation modes. (b) Ethernet / IP through mode.

2.2.1. Configuring the Connector

Both Port A and Port B have one Electrical (RJ-45), one SFP port and one SFP+ connector each. Which one is enabled at any moment is a user decision. The SFP / SFP+ is used to connect the equipment to an optical interface.

The procedure for configuring the connector (RJ-45 or SFP / SFP+) is the following

1. From the *Home* panel, go to *CONFIG*,
   The port setup panel is displayed.
2. Select either *Port A or Port B* to enter in the port specific configuration.
3. Go to *Physical* to enter in the physical settings configuration panel.
4. Select *Connector* to display the available options for the port connector.
   Note: If Connector is configured to SFP, then the actual port in use will depend on the speed and auto-negotiation settings. For example, if auto-negotiation is disabled and the bit rate is forced to *10G*, the selected port will be the 10 Gb/s connector. If auto-negotiation is disabled the port will be the one corresponding tothe 1 Gb/s rate since there is no 10 Gb/s auto-negotiation for optical interfaces.
5. Choose the right connector.
   Note that Port A and Port B do not need to be both optical or electrical at the same time. The test unit is compatible with operation requiring conversion between optical and electrical transmission if all other operation conditions are met.

2.2.2. Using the SFP / SFP+ Ports

The SFP ports are the only choice available for optical tests. They can also be used for electrical tests if compatible SFP / SFP+ are connected but this is usually not necessary due to the attached RJ-45 ports which require no adapters.

Table 2.3: Ethernet SFP Results

Result	Description
SFP present	Shows information about presence of an SFP or SFP+ in the current port.
Transceiver	Displays the current Ethernet interface. Supported interfaces are listed below: • 100BASE-FX: Used for transmission at 100 Mb/s over two MMF in the 1310 optical window. • 1000BASE-SX: Used for transmission at 1000 Mb/s over two MMF operating in the 850 nm optical window. Ranges are usually a few hundred metres. This interface is supported by means an external SFP only. • 1000BASE-LX: Used for transmission at 1000 Mb/s over two MMF or SMF in the 1310 nm optical window. Ranges use to be a few kilometres. This interface is supported by means an external SFP only. • 10GBASE-SR: Used for transmission at 10 Gb/s over two MMF operating in the 850 nm optical window. Ranges up to 300 m depending on the actual optical fibre used as the transmission medium. This interface is supported by xGenius only and it requires an external SFP+. • 10GBASE-LR: Used for transmission at 10 Gb/s over two SMF operating in the 1310 nm. optical window. Standard range is up to 10 km but commercial SFP may offer longer ranges. This interface is supported by Tempo only and it requires and external SFP+. • 10GBASE-TX: Used for transmission at 10 Gb/s over four pairs of Cat. 6, Cat 6a, Cat 7 cable with range up to 100 m. This interface is supported by Tempo only and it requires an special kind of SFP+.
Vendor	If there is an SFP connected to the port, this field shows information about the vendor. This information is recorded within a memory in the SFP when it is manufactured.

Table 2.3: Ethernet SFP Results

Result	Description
Model	If there is an SFP connected to the port, this field shows information about the vendor. This information is recorded within a memory in the SFP when it is manufactured.
TX optical power	In compatible optical SFPs, this field displays the currently transmitted optical power expressed in dBm. Resolution for this result is 0.1 dBm but real result accuracy depends on the specific SFP module.
RX optical power	In compatible optical SFPs, this field displays the currently received optical power expressed in dBm. Resolution for this result is 0.1 dBm but real result accuracy depends on the specific SFP module.
Wavelength	In optical SFPs, this field displays the nominal wavelength used by the light source.

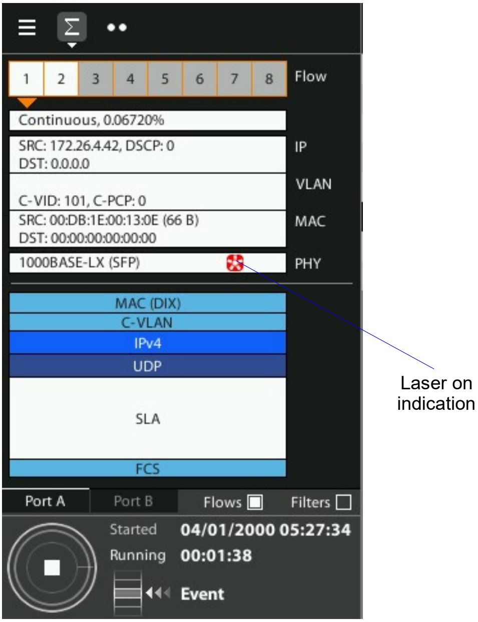
To display the SFP / SFP+ interface information follow these step sequence:

1. From the *Home* panel, go to *RESULTS*,
   The test port results panel is displayed.
2. Select either *Port A or Port B* to enter in the port specific results.
3. Enter in *SFP information* and check the *SFP present*, *Transceiver*, *Vendor*, *Model*, *TX optical power*, *RX optical power* and *Wavelength*.

For security reasons, the optical transmitter is not automatically enabled when the equipment boots up. To switch the optical transmitter on, follow this procedure:

1. From the *Home* panel, go to *CONFIG*,
   The port setup panel is displayed.
2. Select either *Port A or Port B* to enter in the port specific configuration.
3. Go to *Physical* to enter in the physical settings configuration panel.
4. Set *Laser* to *On* to enable the optical transmitter in the current port.
   Note: It is recommended to switch the optical transmitter once the testing has finished.

Current on / off status of the optical transmitter is always available from the *Summary* tab and in the notification area on the top of the screen.



Continuous, 0.06720%

SRC: 172.26.4.42, DSCP: 0
DST: 0.0.0.0

C-VID: 101, C-PCP: 0

SRC: 00:DB:1E:00:13:0E (66 B)
DST: 00:00:00:00:00:00

1000BASE-LX (SFP)

Started 04/01/2000 05:27:34
Running 00:01:38

Laser on indication

Figure 2.2: *Laser on* indication in the Tempo Summary panel.

2.2.3. Configuring Port A and Port B Auto-negotiation Parameters

Many Ethernet ports use auto-negotiation to negotiate speed, duplex operation and other parameters with the peer interface. Ethernet auto-negotiation can be enabled or not in the test unit. If auto-negotiation is enabled, the user decides whether to restrict the available bit-rates. If the user decides to disable auto-negotiation, then the bit rate is forced to a user configurable value.

It should be noticed that Ethernet international standards (and specifically the IEEE 802.3) either does not define any auto-negotiation mechanism for some interfaces or it explicitly forbids not auto-negotiated operation in some interfaces. For example, There is no auto-negotiation for 10 Gb/s interfaces. SFP+ are always configured to a forced 10 Gb/s bit rate in full duplex mode. On the other hand, auto-negotiation is mandatory in 1000 Mb/s electrical interfaces. Auto-negotiation is always enable if this interface is being used.

Table 2.4: Ethernet Auto-negotiation Setup

Setting	Description
Enable	Enables or disables the standard Ethernet auto-negotiation procedure during the connection setup. Auto-negotiation sets the link bit rate, duplex mode, flow control mode without user intervention. Disable Auto-negotiation only if you know that the remote end does not support this procedure or if you want to check link operation without auto-negotiating.
1000-FD	Allows / disallows the interface to negotiate the 1000 Mb/s transmission rate. This is the only choice available if an optical SFP transceiver for 1000BASE-X is attached to the port.
100-FD	Allows / disallows the interface to negotiate the fast Ethernet speed (100 Mb/s) if you are using the RJ-45 port or a compatible electrical SFP for data transmission.
10-FD	Allows / disallows the interface to negotiate the 10 Mb/s transmission rate if you are using the RJ-45 port or a compatible electrical SFP for data transmission.
Clock role	Sets the master / slave clock role in 1000BASE-T interfaces. The available settings for this field are listed below: • *Auto*: The master / slave role designation is automatic and in principle random. • *Master*: The synchronization master role is forced in the interface. This is the right configuration for frequency offset generation or sinusoidal phase modulation generation in Tempo. • *Slave*: The synchronization slave role is forced in the interface. This is the right configuration value for frequency and phase measurements over the interface, including MTIE and TDEV, in the units with the.ability to measure these metrics. The clock role setting makes sense only if the equipment is allowed to negotiate the 1000BASE-T interface over a native RJ-45 port.

Under normal circumstances, the preferred link speed is the highest available. Use *1000-FD*, *100-FD* and *10-FD* settings if you want to analyse the link operation under sub-optimal circumstances. For e example use it to operate at 10 or 100 Mb/s in a link supporting 1000 Mb/s. The general procedure to configure the auto-negotiation in your test unit is as follows:

Table 2.5: Ethernet Auto-negotiation Results

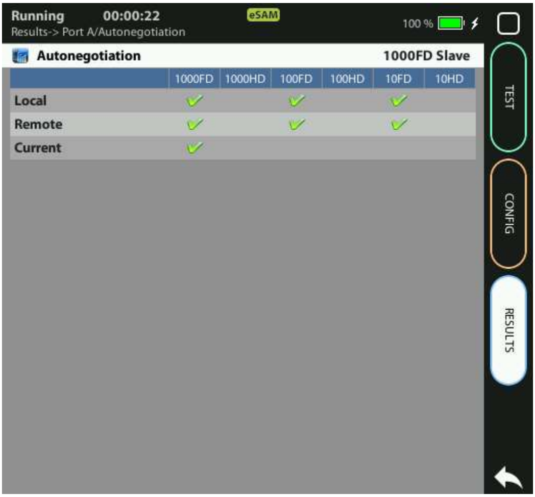
Result	Description
Local	Displays the bit rate and duplex mode supported by the equipment Port A or Port B. If the current connector is the RJ-45, the supported bit rates are 10 Mb/s, 100 Mb/s and 1000 Mb/s (1000FD, 100FD and 10FD). If the connector is set to SFP the supported bit rate is 1000 Mb/s (1000FD).
Remote	Displays the bit rate and duplex mode supported by the remote device connected to Port A or Port B. It is one or several of 1000FD, 1000HD, 100FD, 100HD, 10FD, 10HD.
Current	Bit rate and duplex operation agreed during the auto-negotiation process. It is one (and only one) of the 1000FD, 100FD and 10FD set. If there is more than one compatible interface, the one with higher bit rate is preferred.

1. **From the *Home* panel, go to *CONFIG*,** The port setup panel is displayed.
2. Select either *Port A or Port B* to enter in the port specific configuration.
3. Go to *Physical layer* to enter in the physical settings configuration panel.
4. Go to *Autonegotiation*.
5. Set *Enable* to *Yes* to configure the link speed using auto-negotiation or to *No* to disable auto-negotiation and force the link speed to a fixed value.
6. If you have enabled auto-negotiation in the previous step configure the allowed bit rates through the *1000-FD*, *100-FD* and *10-FD* menus. If auto-negotiation is disabled, set the *Forced bit-rate* to *10*, *100, 1000 or 10 G* from the *Physical layer* menu.
   Note: The 1000 Mb/s rate in electrical interfaces cannot be forced and it is only available through auto-negotiation due to IEEE 802.3 restrictions.The 10 Gb/s cannot be auto-negotiated due to restrictions in the same standard. This bit rate is always forced.

Once the tester has been connected to the network and the right connector type as been configured, follow these steps to check auto-negotiation results:

1. From the *Home* panel, go to *RESULTS*,
   The test port results panel is displayed.
2. Select *Port A or Port B* to enter in the port specific results.

3. Press *Auto-negotiation*
   The auto-negotiation status table for the current port is displayed.
4. Verify which bit rate / duplex modes combinations are supported by the local interface and the remote peer in the *Local* and *Remote* rows. Check the current speed and duplex mode in the *Current* row.



Autonegotiation 1000FD Slave

	1000FD	1000HD	100FD	100HD	10FD	10HD
Local	✓		✓		✓	
Remote	✓		✓		✓	
Current	✓					

Figure 2.3: Calnex Tempo auto-negotiation results panel.

2.3. Entering the Port Local Settings

Ethernet devices do not normally require any configuration to work other than their factory-set MAC address but when the equipment is configured in *IP Endpoint* mode it behaves like any other IP host in the network. That means that the test unit should be able to receive traffic directed to it or transmit test and signalling traffic to other devices. To do that, users should assign an IP profile to each test port. Port A and Port B need an IP address, network mask, gateway address and DNS address to operate.

Table 2.6: Local Ethernet / IP Profile

Result	Description
Ethernet address	This is a read-only field that displays the factory MAC address assigned to the port. The traffic generator supports emulation of MAC traffic from sources other than the factory MAC, but the address displayed here is the real, unique MAC address used in default configuration.

Table 2.6: Local Ethernet / IP Profile

Result	Description
Frame	This menu configures the Ethernet frame properties including encapsulation, VLAN properties. Specifically, the *Frame* has the following settings: • *Encapsulation*: Selects between untagged Ethernet frames (*None*) or IEEE 802.1Q VLAN-tagged frames (*VLAN)*. • *C-VID*: Configures the VLAN identifier when *Encapsulation* has been configured to *VLAN*. Any value within 0 to 4095 is allowed for this field. • *C-VLAN priority*: Configures the VLAN priority bits assigned to the frame. Any value between 0 and 7is allowed for this field. The *Frame* settings apply to all traffic generated by the unit unless it is specified otherwise by the corresponding settings. The *Frame* settings also apply to the traffic received in the test port.
Use DHCP	Defines the procedure used to set the IP profile to the current port. The port IP profile is made up of an IPv4 address, a network mask, an optional gateway address and an optional DNS address. If *Use DHCP* is enabled, then the *Dynamic Host Configuration Protocol* (DHCP) defined in standard RFC 1531 will be used to set the IP profile in the current port.
Static IPv4 address	Is the 32 bit IPv4 address assigned to the local port in decimal, four-dotted format. Addressing scheme used here follows standards RFC 790 and RFC 791. The static addressing is used only if no dynamic address configuration like DHCP is used for the port.
Static IPv4 network mask	Subnet mask used to identify the network address bits and host address bits in the *Static IPv4 address*. The use of the subnet mask is defined in RFC 1219. The subnet mask is entered in decimal, four-dotted format and it must belong to the same network (same network bits) than the current port. The static addressing is used only if no dynamic address configuration like DHCP is used for the port.
Static IPv4 gateway	IP address corresponding to the network device used to send IP packets to external networks. The gateway address is configured in decimal, four-dotted format.

Table 2.6: Local Ethernet / IP Profile

Result	Description
Static IPv4 DNS server	IP address corresponding to the host used for domain name resolution. A DNS server allows the user to identify destinations by alphanumeric domain names rather than numeric IP addresses. The DNS address has to be entered in decimal, four-dotted format.
Leased IPv4 address	Current DHCP-assigned IP address in a decimal four dotted format. This is a read-only field that cannot be directly configured by users This setting makes sense only if *Use DHCP* is enabled.
Leased IPv4 network mask	Current DHCP-assigned network mask in a decimal four dotted format. This is a read-only field that cannot be directly configured by users This setting makes sense only if *Use DHCP* is enabled.
Leased IPv4 DNS server	Current DHCP-assigned DNS server in a decimal four dotted format. This is a read-only field that cannot be directly configured by users. This setting makes sense only if *Use DHCP* is enabled.
Leased IPv4 gateway	Current DHCP-assigned default gateway in a decimal four dotted format. This is a read-only field that cannot be directly configured by users This setting makes sense only if *Use DHCP* is enabled.

In order to configure the IP profile in your test unit follow these steps:

1. From the *Home* panel, go to *CONFIG*,
   The port setup panel is displayed.
2. Select either *Port A or Port B* to enter in the port specific configuration.
3. Enter in *Local profile*.
4. Configure the encapsulation to *None* or *VLAN* depending on where the equipment is to be connected. If the encapsulation is set to *VLAN*, configure the *C-VID* and *C-VLAN* priority to the correct values for your network.
5. Decide whether you want to configure the local IP profile with the help of the DHCP protocol or you want to statically set these profiles by means the *Use DHCP* control.
   If you have enabled DHCP wait for the tester to get an IP profile from a DHCP server. If DHCP is not enabled, enter a valid *Static IPv4 address*, *Static IPv4 network mask*, *Static IPv4 gateway* and *Static IPv4 DNS address*.
   Note: For Port B, you only need to enter a valid IPv4 address and network mask.

2.4. Using Pluggable Hardware Modules (PHMs)

Pluggable Hardware Modules (PHMs) are a way to extend the default Tempo functionalities. There are currently five different PHMs. The Datacom Test Module can be used for datacom testing, IEEE C37.94 test module is a dual-port IEEE C.37.94 module, the ITU-T G.703 module can be used for ITU-T G.703 co-directional, contra-directional and centralized tests, the Voice frequency test module is an analog (VF) test module and E1 / T1 port test module adds and additional E1 / T1 test port. More PHMs can be designed in the future supporting more functions, interfaces and tests.

PHMs are hot pluggable:. Users are allowed plug or unplug modules at any time. If the correct software license is installed in the test unit, the menus requiring the PHM will be displayed in the regular menu structure but when the user enables any option related with the PHM a warning (yellow) indication will be displayed on the top of the screen to inform that the PHM is not attached. The warning message includes the PHM name. For example, if the *C37.94 endpoint* mode is enabled but the IEEE C37.94 test module is not connected to the unit then a *PHM* warning message will be displayed.

2.5. Using the Traffic Reflector

You can configure the test unit ports in loopback mode so that the traffic they receive is forwarded toward their originator. This is very useful in many test and measurement applications where the traffic generator receives the transmitted frames back and runs some kind of analysis over this traffic requiring correlation between received and transmitted frames. Examples of this are BER and latency analysis.

Table 2.7: Local Ethernet / IP Profile

Result	Description
Loop mode	The loop mode determines which fields within the Ethernet frame or the IP datagram are swapped before forwarding. Is one of the following ones: • *Physical loop*: Loops frames without other alteration than pulse shape regeneration. This mode may cause problems if it is used in a bridged network. • *MAC loop*: Swaps source and destination MAC addresses before forwarding the frame. This is the correct mode to be used in bridged networks. • *IP loop*: It operates in the same way that the *MAC loop* mode but is swaps source and destination IP addresses as well. This is the correct mode to be used in routed networks. The *IP loop* mode is not available in *Ethernet endpoint mode*.

Table 2.7: Local Ethernet / IP Profile

Result	Description
	• *UDP loop*: It works in the same way that the *IP loop* mode but it swaps source and destination UDP ports as well. This mode can be used if there are network devices working at the transport layer like for example firewalls or NAT routers. The *UDP loop* mode is not available in *Ethernet endpoint* mode.
Traffic to loop	Configures which frames are looped in the current test port. The available configurations are: • *All frames*: Loops all frames received in the test port. • *Filtered frames*: Loops frames matching any of the eight receiving filters available for configuration. All non-matching frames are discarded. Use this option if you need a tight control on the looped frames.
Loop broadcast frames	Chooses whether to loop Ethernet broadcast frames. If broadcast loop is disabled, all frames with destination MAC address set to *FF:FF:FF:FF:FF:FF* are discarded. Use this setting if you want to avoid Ethernet broadcast frames to proliferate and potentially flood the network.
Loop ICMP packets	Chooses whether to loop ICMP packets. If ICMP loop is disabled, all ICMP frames (IP protocol number 1) will be discarded. Use this setting to avoid ICMP packet proliferation in the network.

It must be remembered that while a port is operating in loopback mode (or even in monitor mode) it still replies to some basic network protocols like ARP or ICMP echo request (ping) messages. Of course, ARP and ICMP echo requests are also looped if the port is configured to do so.To enable the loopback mode configure Port mode to

Loopback in any of the L1 endpoint, Ethernet.endpoint and IP endpoint modes (See section 2.1) and configure the *Loopback* setting menu.

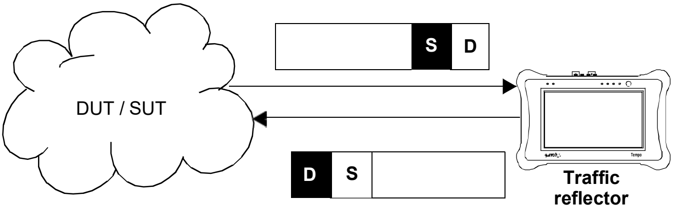


Figure 2.4: This figure illustrates the loop-back operation (*MAC loop*). Source and destination addresses are swapped so that they can be processed in the normal way by intermediate switches.

2.6. Testing with an External Clock Reference

Some tests performed by Tempo require a clock reference. Moreover, it is possible that the user is interested in setting the transmission timing source of Port A / Port B transmitters to something different to the default configuration. Clock reference configuration for tests that require an external timing source is carried out through the *Reference clock* menu. The source timing candidates are the following ones:

Table 2.8: Reference Clock Panel

Result	Description
Input clock	Enables the user to choose between different reference clock inputs, including the internal clock input. The specific clock input list depends on the hardware configuration.
Output clock	Enables the user to choose between different clock reference outputs.These outputs could be used to synchronize an external equipment, including a second Tempo, with the test unit. The available outputs depend on your hardware configuration.

Table 2.8: Reference Clock Panel

Result	Description
Internal reference status	Displays information about the internal clock reference when it is free running, locked to an external reference or in holdover. • *Free run*: The clock reference input is internal and the oscillator is free running without any external discipline.The oscillator will exhibit a frequency offset that will depend on the oscillator type, aging, last calibration date and temperature. A free running oscillator may still be suitable to run some frequency tests but it will generally unsuitable to perform measurement related with time / phase. • *Do not use*: The oscillator has been configured to be disciplined to an external clock reference but the locking process is still starting. When the reference reports the “Do not use” status large variations in phase or frequency may happen and therefore the equipment is not yet ready for any test requiring accurate synchronization. • *Not sync*: The internal oscillator is in the process of acquiring the frequency and phase from the external clock reference. Large variations in the internal oscillator phase and frequency may happen during this period and the equipment is not ready for any test for this reason. • *Locking*: The internal oscillator is in the last phase of the locking process. No sudden phase changes are expected in this state. In this status, the unit becomes ready for all tests not requiring the maximum accuracy degree. • *Holdover:* The unit has been previously locked to an external time or phase reference but now the reference input is not being used. The unit keeps an accurate reference frequency and phase for a limited period of time. When the unit is operating in holdover mode it is still ready for testing even if no external clock reference is available. • *Error reference*: For some reason, the local oscillator is not able to finish with the locking sequence. This message should never be displayed under normal operation.

Table 2.8: Reference Clock Panel

Result	Description
GNSS receiver	Enables access to the GNSS configuration menu and shows information about the GNSS receiver status. These are • *No data*: There is no connection between the test unit and the GPS / Glonass receiver or the receiver is not generating any data. • *Acquiring fix*: The GNSS receiver has not yet acquired position and time. Achieving this data may take a few seconds. The equipment may fail to achieve the fix if there are not enough satellites in sight. • *Waiting for PPS*: The GNSS receiver has acquired position and time and it is reporting this information but it is not yet generating the 1 PPS signal required for a correct assessment of the position / time. • *Synchronizing to PPS*: The GNSS receiver is now reporting position and time and generating a 1 PPS. The unit is acquiring this information. • *Synchronized to GNSS*: The test unit is tracking the GNSS signal. The time scale reported by the GNSS constellation is being used. For example the GPS time is 19 seconds behind TAI. • *Synchronized to UTC*: The test unit is tracking the GNSS signal. UTC time scale is used. Once the GNSS status is reported the unit cannot get the UTC time unless the TAI-UTC second count is known. This data is also reported by the satellite system and it takes some time before the information is acquired. The GNSS configuration menu is greyed out unless the GNSS clock reference input is configured in *Input clock*.
PPS / ToD input interfaces	Menu that configures and reports status of 1 PPS, 1 PP2S and ToD clock references outputs. Configuration of these interfaces is limited to a custom incoming cable delay compensation. The displayed status information corresponds with the ToD format (*ITU-T G.8271*, *NMEA*, *China Telecom*). This menu entry is enabled only if Input clock is configured to any of *1 PPS (REF IN)*, *1 PP2S (REF IN)*. *ToD (REF IN/ OUT)*.

Table 2.8: Reference Clock Panel

Result	Description
PPS / ToD output interfaces	Menu that configures and reports status of 1 PPS, 1 PP2S and ToD clock reference outputs. Configuration of these interfaces is limited to a custom outgoing cable delay compensation and the ToD format (*ITU-T G.8271*, *NMEA*) to be configured at the output.
IRIG-B input interfaces	Menu that configures an IRIG-B clock reference input in the unit. IRIG-B time codes are conceptually similar to ToD interfaces but in IRIG-B, time, date, time scale and any other information related with timing is embedded in a single electrical signal. The test unit is able to decode IRIG-B clock reference both from balanced (RJ-45) and unbalanced (SMB) interfaces.
IRIG-B output interfaces	Menu that configures an IRIG-B clock reference output in the unit. IRIG-B time codes are conceptually similar to ToD interfaces but in IRIG-B, time, date, time scale and any other information related with timing is embedded in a single electrical signal. The test unit is able to provide IRIG-B clock reference outputs both in balanced (RJ-45) and unbalanced (SMB) interfaces.
Clock / PCM input interfaces	Configures a clock (1544 kHz, 2048 kHz, 5 MHz or 10 MHz) or a PCM (1544 kb/s, 2048 kb/s) reference input.received in a balanced (RJ-45) interface
Clock / PCM output interfaces	Configures a clock (1544 kHz, 2048 kHz, 5 MHz or 10 MHz) or a PCM (1544 kb/s, 2048 kb/s) reference input.received in a balanced (RJ-45) interface
Oscillator	Opens the oscillator configuration menu.This menu enables users to get information about the oscillator status and force the holdover operation.

- *Internal*: The test unit clock reference is configured to use the timing from an internal oscillator. This oscillator is a temperature-controlled crystal oscillator (TCXO) which provides a frequency accuracy better than ±2.0 ppm. The user can optionally replace the TCXO by an oven-controlled crystal oscillator (OCXO) or a Rubidium oscillator which provide higher frequency accuracy than the TCXO.
- *Clock/PCM (REF IN/OUT)*: The clock reference is derived from an external PCM or clock signal. Options included in this set are 2048 kHz, E1,1544 kHz, T1, 5 MHz and 10 MHz. This signal is received through the REF IN/OUT RJ-45 port. For this reason, this option is available only if a clock reference output has not been previously configured over the same port.

- *ToD (REF IN/OUT)*: Clock reference input derived from an external 1 PPS / ToD interface received through the RJ-48 REF IN/OUT port. There are three ToD protocols supported: NMEA, China Telecom, ITU-T G.8271. These are automatically detected.
- *PPS (REF IN/OUT)*: The clock reference is derived from an external 1PPS (1 pulse every second) or 1PP2S signal (1 pulse every two seconds) received through the RJ-48 REF IN/OUT port located in the test connector panel. PPS signal type is automatically detected and it doesn't require user intervention.
- *PPS (REF IN)*: The clock reference is derived from an external 1PPS (1 pulse every second) or 1PP2S signal (1 pulse every two seconds) signal received through the PPS RX SMB port located in the test connector panel. PPS signal type is automatically detected and it doesn't require user intervention.
- *Ethernet (Port A) / Ethernet (Port B)*: A Synchronous Ethernet signal recovered from Port A (or Port B) is used as the external clock reference. The equipment may fail to synchronize to a conventional (asynchronous) Ethernet input depending on the specific frequency offset of the input compared with the free running frequency of the internal clock. For the particular case of a 1000BASE-T input, the interface must be forced to an slave role before the input can be used as a synchronization reference (See section 2.2.3).
- *IRIG-B (REF IN/OUT)*: The clock reference is is derived from any of the IRIG-B time codes available in the unit. The signal is received through the RJ-48 REF IN/OUT port located in the test connector panel. Most of the parameters related with IRIG-B transmission are automatically detected (See section 2.6.1).
- *IRIG-B (REF IN)*: The clock reference is is derived from any of the IRIG-B time codes available in the unit. The signal is received through the SMB REF IN port located in the test connector panel. Most of the parameters related with IRIG-B transmission are automatically detected (See section 2.6.1).
- *GNSS*: Actually, this is not a clock reference input but a RF input used by the optional built in GNSS receiver to internally generate a timing signal that improves the internal oscillator default performance when operating in free-running mode (See section 2.6.2).

Table 2.9: Oscillator Settings and Status

Result	Description
Oscillator status	For a proper operation of your Tempo test unit, the oscillator status should always be *Calibrated*. Not calibrated oscillators may not be able to track correctly an external reference and they could generate large frequency offsets when they operate in free running mode. Contact Calnex customer service or your Calnex local representative if your unit is showing something different to *Calibrated* in this field.

Table 2.9: Oscillator Settings and Status

Result	Description
Oscillator type	Supported oscillator types are TCXO, OCXO and Rubidium. These are the basic properties and differences between all three possibilities: • *TCXO*: This oscillator has a frequency offset of the order of 1 ppm. It is well suited for all standard test applications not including one way latency measurements or synchronization testing involving GNSS, 1 PPS or PTP interfaces. It does not support operation in holdover mode. • *OCXO*: Standard oscillator for applications involving GNSS, 1 ppm or PTP interfaces. The frequency offset is of the order of 0.1 PPS. The long term stability of OCXOs are better than in TCXOs and for this reason they can be used in some holdover applications. • *Rubidium*: It offers better accuracy than OCXOs both in terms of phase and frequency stability. This oscillator is also better shielded against temperature variations than the OCXO. The main advantage of Rubidium oscillator is its excellent holdover performance. Rubidium units are best suited for synchronization tests requiring high accuracy degree both in locked or holdover states.
Oscillator lock status	This field provides information about the disciplining status corresponding with the internal clock. It can be one of the following: • *Warm up*: Shows that the oscillator is still initializing. No accurate frequency or phase could be expected when the oscillator is still in this mode. The *Warm up* status could last for a few minutes. • *Locking*: The oscillator has finished the initialization sequence and it starts tracking the external reference frequency and phase. The objective of this state is to minimize the phase and frequency difference between the local oscillator and the reference. During the *Locking* period the oscillator frequency and phase may not be accurate or they may change quickly. For this reason no test should be run in *Locking* state. The *Locking* status lasts for around 20 minutes in Rubidium units and 5 minutes in OCXO units.

Table 2.9: Oscillator Settings and Status

Result	Description
	• *Fine locking*: The unit is still trying to minimize the phase difference between the internal oscillator and the reference but no sudden phase changes are expected in this state. When the unit achieves the *Fine locking* status, it becomes ready for all tests not requiring the maximum accuracy degree. The Fine locking state lasts for a few seconds in OCXO units and about four hours in Rubidium units. • *Locked*: The unit cannot reduce the frequency and phase difference between the reference clock and the local oscillator any more and it just tracks the output to keep the differences to the minimum. In this situation, the test error is minimum and therefore the unit is ready for any measurement. • *Holdover:* The unit has been previously locked to an external time or phase reference but now the reference input is not being used. The unit keeps an accurate reference frequency and phase for a limited period of time. When the unit is operating in holdover mode it is still ready for testing even if no external clock reference is available. • *Holdover time out*: The unit has been working in holdover for longer than programmed in the *Holdover duration* field. The local oscillator frequency and phase are not reliable when working the holdover is timed out. • *Free running*: The local oscillator is not disciplined and it is operating on its natural oscillation frequency. How accurate this frequency is depends on which oscillator is being used (TCXO, OCXO or Rubidium) and how well the oscillator is calibrated. The phase and time supplied by a free running oscillator are not reliable. • *Reference error*: For some reason, the local oscillator is not able to finish with the locking sequence. This message should never be displayed under normal operation.
Force holdover	Puts the OCXO or Rubidium oscillator in holdover mode. When this mode is set, The user is allowed to physically unplug the external clock interface. The equipment, will try to generate accurate phase and frequency on its own based on previous data from the reference. The holdover mode is not available in TCXO units.

Table 2.9: Oscillator Settings and Status

Result	Description
Holdover elapsed time	It accounts for the time from the beginning of the holdover period. This value should always be smaller than the *Holdover duration*. If the *Holdover elapsed time* becomes higher than the Holdover duration then the test unit goes to a holdover timed out state.
Holdover duration	This field could be used to configure the amount of time required to declare a holdover timed out. The default holdover duration period is 24 hours.

The procedure to configure the clock reference input in your Tempo unit is detailed in the following steps.

1. From the *Home* panel, go to *CONFIG*,
   The port setup panel is displayed.
2. Go to *Reference clock*.
3. Configure *Input clock* to one of *Internal*, *Clock/PCM (REF IN/OUT)*, *ToD (REF IN/OUT)*, *PPS (REF IN/OUT)*, *PPS (REF IN)*, *Ethernet (Port A)*, *Ethernet (Port B), GNSS*, *IRIG-B (REF IN/OUT)* or *IRIG-B (REF IN)*.
4. If you have chosen *Clock/PCM (REF IN/OUT)* in the previous step, configure *Clock/PCM Input, Connector and Connection mode* from the *Clock/PCM input interfaces* menu. If you have chosen *PPS (REF IN/OUT)*, *PPS (REF IN), ToD (REF IN/OUT) IRIG-B (REF IN/OUT)* or *IRIG-B (REF IN)*. configure the *Input reference delay* and other PPS / ToD / IRIG-B related parameters (See section 2.6.1). If you have configured GNSS in the previous step, configure *Antenna cable delay*, *Active GNSS* and other GNSS related parameters from the GNSS receiver menu (See section 2.6.2),

2.6.1. Using PPS / ToD, IRIG-B and Frequency References

Tempo includes three different kinds of clock reference. Every clock reference type has different features and they are used for different applications.

- *Frequency references*. This class includes the 2048 kHz, E1, 1544 kHz, T1, 5 MHz and 10 MHz. Locking the unit to any of these references is very fast. It takes only a few seconds even in Rubidium units. The disadvantage is that holdover from frequency references is not supported Frequency references are also unsuitable for time and latency tests but they are good for accurate frequency offset and drift tests and wander (TIE, MTIE, TDEV) tests.
- *Time references.* Includes the ToD and the IRIG-B references. The ToD is made up of a 1 PPS that provides accurate phase timing and a protocol that distributes the time in an absolute time scale such as TAI or UTC. The ToD can be used to measure TE in any interface including, PTP, 1 PPS and frequency. IRIG-B has

some points in common with ToD references but it has the ability to be transmitted over both coaxial and balanced interfaces such as RS-232 or RS-422.

- *Phase references*. They are the 1 PPS and the 1 PP2S references. Phase references offer something that is in between time and frequency references. They can be used to measure TE in other phase references such as 1 PPS and 1 PP2S but they cannot do the measurement with time protocols such as IEEE 1588 / PTP.

Table 2.10: PPS/ToD Input Interfaces Options

Parameter	Description
Input reference delay	Compensates the delay added by the physical media propagation delay when the *Input clock* reference is set to *PPS (REF IN/OUT)*, *PPS (REF IN) or ToD (REF IN/OUT)*.
Input ToD status	Displays information about the ToD protocol detected in the clock reference input. It could be *No ToD*, if the ToD format is not recognised or *G.8271*, *NMEA* or *China Telecom* when any of these ToD protocols is detected
Input PPS status	This field informs about the detected PPS signal type. It could be *1PPS* (1 pulse per second) or *1PP2S* (1 pulse every two seconds). It also displays a *No PPS* indication when no valid PPS signal is detected.
Input level	Configures the expected signal amplitude in unbalanced PPS ports. It could be either 3.3 V or 5 V.
Input impedance	Configures the input impedance in unbalanced PPS inputs. In unbalanced (SMB) inputs the impedance could be 50 Ω or high impedance.

The parameters to be configured are also different depending on the clock reference class. Time and phase references require an adjustment to compensate for the latency in the patch cable from / to the DUT. The same setting applies both to phase and time references. Frequency (and sometimes also PPS) references require an impedance configuration. Setting a high impedance value enables monitoring applications without disturbing the line and the nominal impedance can be used to avoid reflections when the test unit is connected in endpoint mode.

Table 2.11: IRIG-B Input Interfaces Options

Parameter	Description
Input IRIG-B status	Compensates the delay added by the physical media propagation delay when the *Input clock* reference is set to *IRIG-B (REF IN/OUT)* or *IRIG-B (REF IN)*.

Table 2.11: IRIG-B Input Interfaces Options

Parameter	Description
Modulation	Configures the IRIG-B signal modulation and encoding in a clock reference input. There are three possibilities: • A pulse width encoding (*Pulse width code (0)*) corresponding with the '0' identifier from the standard. • Amplitude modulated time code (*Sine-wave, AM (1)*) corresponding with the '1' identifier. • Manchester encoded signal (*Manchester modulated (2)*), which is identifier '2'. Amplitude modulated time codes are available only in unbalanced ports (SMB connector). Pulse width and Manchester time codes are available both over balanced and unbalanced ports.
Frequency	Configures the carrier frequency in modulated time codes. If the pulse width encoding is used then the only value for this parameter is *No carrier (0)*, which has identifier '0' from the standard. For Manchester modulated signals, the carrier frequency is statically set to *1khz (2)*, corresponding to a 1 kHz modulation (identifier 2). Amplitude modulated codes accept a carrier frequency of 1 MHz (*1 MHz (5)*) which correspond with identifier 5.
Coded Expression	Describes the time code words used within the IRIG-B frame. It is a combination of encoded information providing details about time. Some of these encoded words are optional and one of them, the BCD Time-of-Year (*bcdtoy*), is mandatory. The optional codes are the *Straight Binary Seconds-of-day* (SBS), the *BCD Year* code, which encodes the current year, and the *Control Functions* (CF) that encode various control, identification or other special purpose functions.
Gain	Applies a gain of 0 dB, 6 dB, 12 dB or 18 dB to amplitude modulated inputs.
Level	Configures the expected signal amplitude in pulse width and Manchester inputs over unbalanced (SMB) ports. It could be either 3.3 V or 5 V.

Table 2.11: IRIG-B Input Interfaces Options

Parameter	Description
Impedance	Configures the input impedance in IRIG-B inputs. In unbalanced (SMB) inputs the impedance could be 50 Ω or high impedance. However, in AM inputs there's the additional 600 Ω to be added to the previous list. In IRIG-B outputs the impedance cannot be configured with the exception of AM signals over unbalanced (SMB) connectors. In this case, the impedance could be either 50 Ω or 600 Ω.
Input reference delay	Configures the cable delay for the interface in nanoseconds. Keeping all delay sources under control in phase and time references is important to make sure that the signal significant instants are the same in all points in the network. The cable delay compensation applies both to ToD reference inputs and outputs.

GNSS has not been included in the previous description but from the point of view of the functionality it offers is equivalent to a ToD reference. There are some points specific about GNSS references: Timing is generated from one or various satellite constellations and information about geographical position and not only time is received. For this, GNSS references have their own configuration menu (See section 2.6.2).

Table 2.12: Clock/PCM Reference Input Interfaces

Parameter	Description
Clock/PCM input	Configures the Clock or PCM reference input interface: • *2048 kHz (Port Ref. In/Out)*: The clock reference is derived from an external ITU-T G.703 2048 kHz signal. This signal is received through the balanced RJ-48 Ref. In / Out port. • *E1 (Port Ref. In/Out)*: The clock reference is derived from an external ITU-T G.703 2048 kb/s signal. This signal is received through the balanced RJ-48 Ref. In / Out port. • *1544 kHz (Port Ref. In/Out)*: The clock reference is derived from an external 1544 kHz signal. This signal is received through the balanced RJ-48 Ref. In / Out port. • *T1 (Port Ref. In/Out)*: The clock reference is derived from an external ITU-T G.703 1544 kb/s signal. This signal is received through the balanced RJ-48 Ref. In / Out port. • *5 MHz (Port Ref. In/Out)*: This is a 5 MHz unipolar clock. Accepts square or sinusoidal signal received through the RJ-48 Ref. In / Out port.

Table 2.12: Clock/PCM Reference Input Interfaces

Parameter	Description
	• *10 MHz (Port Ref. In/Out)*: This is a 10 MHz unipolar clock input. Accepts square or sinusoidal signal received through the RJ-48 Ref. In / Out port.
Connector	Configures the port connector in a Clock / PCM reference input. Since all references of this type are currently received through the balanced RJ-48 Ref. In / Out port, connector setting is not required.
Connection mode	It configures the input / output impedance of the clock inter- face where the *Port C* is going to be connected. The availa- ble configurations for this field are: • *Endpoint*: This connection represents a network termination point with the nominal impedance (75 Ω for the unbalanced port and 120 Ω for the balanced one). The expected attenuation is the theoretical cable attenuation which increases with the frequency square root. • *-20 dB monitor*: 20 dB protected monitoring point. This is a connection point that is isolated from the network and it is specially suited for monitoring purposes. A flat attenuation of 20 dB is expected for these points.

2.6.2. Configuring the Built in GNSS Receiver

Tempo units may optionally be equipped with a built in GNSS receiver. These units have a SMA female connector suitable for connecting an external antenna. Units are also supplied with a compact GNSS antenna with 5 m of coaxial cable plus a 10 m extension cable.Using a different antenna is possible as long as the specifications of the GNSS module are taken into account.

The GNSS interface can be used to synchronize the system time with a satellite constellation but in certain test units, some results may depend on the GNSS timing source. It this case, the test application may enable the GNSS reception on its own. In both cases, the GNSS state can be verified through the same *Clock reference* submenu. To display the GNSS status follow this procedure.

1. Attach the GNSS antenna to the unit. Make sure that the antenna sees as much of the sky as possible. The unit may fail to achieve synchronization if there are not enough satellites in sight. Some tests may loss accuracy if the number of satellites in sight is reduced.

1. From the *Home* panel, go to *CONFIG*,
   The port setup panel is displayed.
2. Go to *Reference clock*.
3. Configure the clock reference input to *GNSS*.

4. Go to *GNSS receiver*.
5. Check the values of *GPS status*, *Satellites received*, *Satellites used*, *PDOP and TDOP.*

Table 2.13: GNSS Receiver Options

Parameter	Description
Antenna cable delay	Compensates the delay added by the physical media when the GNSS signal propagates from the antenna to the receiver.
Active GNSS	Configures the active GNSS constellations. Supported values are: • *GPS*: Enables the *Global Positioning System* in the equipment. This is the satellite constellation managed by the US government. • *Glonass*: Enables the *Global'naya Navigatsionnaya Sputnikovaya Sistema* (GLONASS) constellation, that constitutes the Russian alternative to GPS. • *BeiDou*: Enables BeiDou in the test unit. BeiDou is the Chinese positioning system alternative to the North-American GPS. • *Galileo*: Enables the European Galileo system in the test unit. Depending on the hardware configuration of your particular unit, some of these constellations may not be available for configuration. It is possible to enable two or more simultaneous constellations at the same time. In this case, the satellites for the selected constellations will be simultaneously used.
PPS timing reference	Configures which GNSS timing reference is used as a timing source for the local oscillator. It could be set to *GNSS*, *UTC* or automatic (*Auto*) The recommended value for this setting is *Auto*.

Table 2.13: GNSS Receiver Options

Parameter	Description
GNSS status	Displays the current status of the NMEA interface used for communication with the built in GPS / Glonass module or an external GPS receiver connected to the unit through a 1 PPS / ToD interface. The possible values of *GPS status* are listed below: • *No data*: There is no connection between the test unit and the GPS / Glonass receiver or the receiver is not generating any data. • *Acquiring fix*: The GPS / Glonass receiver is generating NMEA data but it is still not synchronized. Achieving synchronization may take some time. The equipment may fail to achieve synchronization if there are not enough satellites in sight. • *Waiting for PPS*: The GNSS receiver has acquired position and time and it is reporting this information but it is not yet generating the 1 PPS signal required for a correct assessment of the position / time. • *Synchronized To GNSS*: The GNSS receiver is reporting that it has achieved synchronization from the timing data received from the satellite constellations. This is a required condition before the system time becomes locked to the GNSS time.
Antenna power supply	Enables or disables antenna powering through a DC voltage of a nominal value of 5 V. If the antenna power is disabled, then it is necessary to make sure that the antenna is powered through an alternative method. It is recommended to check compatibility between the antenna and the tester before turning the powering voltage on.
Antenna detected	Displays a warning message when no antenna presence is detected. Antenna presence detection is based on the detection of power dissipation in the antenna interface and hence it works only if the antenna power supply is switched on.
Satellites received	This is a read only field that displays the number of satellites on sight. These satellites may correspond to any of the constellations currently enabled.

Table 2.13: GNSS Receiver Options

Parameter	Description
Satellites used	This field shows the number of satellites actually used by the test unit. One satellite may be on sight but it may not be used by the unit for different reasons. The *Satellites used* parameter is the only one relevant to rate the accuracy of the GNSS-derived timing reference
PDOP	Some tests may require a minimum number of satellites or an specific satellite geometry to achieve the required accuracy level. The Position Dilution of Precision (PDOP) gives information about how good is the current satellite geometry to achieve an accurate position estimate. The PDOP is a positive number. The smaller the number, the better is the accuracy. A minimum value of PDOP of 1.5 is recommended to get accurate results in critical tests.
TDOP	Time Dilution of Precision (TDOP). This parameter gives information about how good is the current satellite geometry to achieve an accurate time estimate.
Fixed-position mode	This is the menu that enables the user to configure the fixed GNSS receiver fixed position mode. In this mode the equipment uses given spacial GNSS coordinates (longitude, latitude, altitude) in order to achieve maximum accuracy in the time estimate.
Leap seconds (TAI - UTC)	Reports the current time offset between TAI and UTC. This value is currently set (February 2019) to 37 seconds butthis value changes from time to time as new leap seconds are added to the UTC time scale. The TAI to UTC offset is retrieved from the GNSS constellations without user intervention. This is, therefore a read only field.

You can also actively configure the Tempo GNSS receiver. Some settings are not mandatory but the increase in accuracy it could be obtained in this way is quite important. This is the required procedure:

1. From the *Home* panel, go to *CONFIG*,
   The port setup panel is displayed.
2. Go to *Reference clock*.
3. Go to *GNSS receiver*.
4. Configure the Antenna cable delay to compensate for the distance between the receiver and the antenna.
5. Optionally, enable or disable any of the *GPS*, *GLONASS*, *BeiDou* or *Galileo* constellations through the Active GNSS setting.

6. Go to *Fixed-position mode*.
7. Optionally, adjust the *Position averaging time* and enable position averaging by configuring *Fixed-position mode* to *Auto-average*.
   The *Fixed-position status* field now displays *Averaging*
   Note: At least one hour of position averaging is required for a reasonable accuracy.
   Note: The position averaging procedure should be run only once as long as the test unit geographical location is not changed. The unit checks any change in position (longitude, latitude, altitude) every time it is connected to a GPS antenna. If a change in the coordinates is detected, then an error message is displayed in the status field and the mode is disabled.
8. Wait to the *Fixed position status* to become *Active*. The unit is now ready for testing.
   Note: Theoretically, testing could start before the end of the position averaging process. The improved time estimation due to this function would be automatically applied starting from the end of the auto-averaging process.

2.6.3. Using the Holdover Mode

Tempo units carrying OCXO and Rubidium oscillators can operate in holdover mode. They can be disconnected from the clock reference input and they still keep accurate frequency and phase for a period of time that ranges from a few minutes for OCXO units or a few hours in Rubidium units. The holdover mode cannot be used in TCXO units.

The holdover mode is useful when, for some reason, there is not a suitable clock reference that could be used in the test site In this case, the equipment could be synchronized to a GNSS or any other clock source far from the test site and driven to holdover.The results are accurate within a period of time as long as the test unit is not restarted

To enable the holdover operation in Tempo, follow these steps:

1. Connect and configure the clock reference input in your test unit to *GNSS* or any of the IRIG-B, 1 PPS, 1 PP2S or ToD interfaces (See section 2.6).
   Note: Holdover from a frequency reference is not supported.
2. For optimum performance, in Rubidium units, wait for at least two hours once the test unit is locked to the clock reference input. In OCXO units no additional waiting time is necessary once the equipment is locked.
   Note: Theoretically, the unit could the driven to holdover when it is still in a *Fine locking* state but the accuracy level will be lower if this is done.
3. From the *Home* panel, go to *CONFIG*,
   The port setup panel is displayed.
4. Go to *Reference clock*.
5. Go to oscillator.

6. Optionally, configure *Holdover* duration to the time you want to keep the unit in holdover. The unit will go to a Holdover timeout once this time is reached and frequency / time traceability will be lost.
7. Configure *Force holdover* to *Yes*
   An small *H* is displayed in the screen to show that the unit has entered in holdover.
8. Optionally, unplug the clock reference input from the test unit.
   The REF LED now displays the red colour. The unit is ready for testing.

In Rubidium units, it is possible to recover from a holdover without restarting the oscillator control loop from the beginning. This is the right procedure to do that:

1. Plug a GNSS or 1 PPS clock reference to the right connector in your Tempo tester.
2. Make sure that the equipment is receiving the reference (green REF LED)
3. From the *Home* panel, go to *CONFIG*,
   The port setup panel is displayed.
4. Go to Reference clock.
5. Configure *Force holdover* to *No*
   Oscillator lock status will go to *Warm up* or *Fine locking*, depending on how far is the clock reference from the current local oscillator frequency and phase.

Holdover is important when accurate timing is required to run a test but the reference is not available in the location where the test is to be run. Typical examples are data centres in basements or in rooms without windows. These conditions make it difficult to use GNSS, which is the most universally available reference. The holdover mode has to be used carefully, however. Some oscillators can be set to “remember” frequency and phase for a period of time once they have been disconnected from the reference but sooner or later they will drift to their natural oscillation frequency and the holdover will resemble more and more to the free running operation. Tempo users must be aware of the performance level they could expect from the test unit to decide which tests are feasible and which are not.

For example, a Tempo with an internal Rubidium oscillator, is configured in holdover. The specification is that the phase error will be less than 1000 ns after 24 hours, which corresponds with an average frequency offset of1.2 x 10^{-11} for the 24 hour measurement period. If the holdover period is extended for longer, then the frequency will drift and the offset will increase to approach the oscillator natural frequency. This frequency depends on factors such as the aging.

The expected phase error (1000 ns) and frequency error (2 x 10^{-11}) must be compared with the expected test results: PRTCs (ITU-T G.8272 clocks) must supply an accuracy level in terms of TE better than 100 ns and the PRC (ITU-T G.811) accuracy in terms of frequency offset is 1 x 10^{-11} or better. It is clear that Tempo configured in holdover mode will not provide the accuracy level required to assess compliance with the G.7272 and G.811 frequency and phase requirements. On the other hand, ITU-T

G.813 requires a frequency offset smaller or equal than 4.6 ppm for oscillators claiming compliance with this standard and ITU-T G.8271.1 specifies an MTIE of the order of hundreds of nanoseconds for a test period of 10000 seconds. For these test cases, holdover operation may be appropriate.

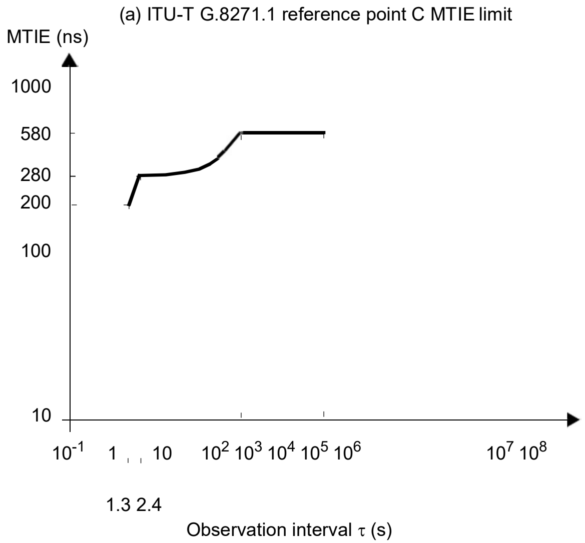


Figure 2.5: ITU-T G.8271.1 MTIE mask to be verified at the input of the T-TSC

All previous examples are based in a comparison between the expected test error and the magnitude to be measured. Sometimes, the limiting factor could be not the magnitude to be measured but the test resolution or other error sources. An example of this is latency measurement in E1 and T1 interfaces. The expected accuracy level in these tests is two or three microseconds with perfect timing. For this reason, an error of hundreds of nanoseconds hardy matters.

Aging is not the only factor that limits the accuracy of an oscillator. Magnetic fields, air flows, mechanical vibrations and among all them temperature have the capacity to modify the oscillator frequency.

For the example of the Rubidium Tempo, the holdover accuracy of 1000 ns in 24 hours applies only to operation with temperature changes within ±2 ºC. If the temperature range changes in a range of ±10 ºC, then the error becomes closer to 3000 ns.

There are some interesting facts related with errors induced by temperature variations. We could try to describe two typical situations to illustrate these facts:

1. A test is to be done in a room where access to GNSS is not possible and there is no other signal that could be used as an alternative reference input. Tempo is synchronized in a different room at a different temperature and then

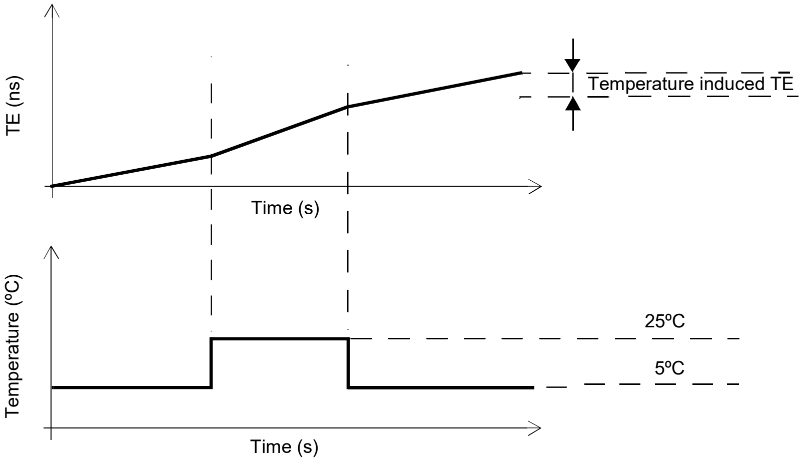


Figure 2.6: Temperature induced TE when the equipment is operating in holdover.

moved to the test location. If the temperature difference in both rooms is larger than four degrees Celsius then the 1000 ns holdover performance could not be guaranteed. Not only phase and time measurements will be affected; the frequency in the test location will also be different to the room where the equipment was synchronized.

2. The test unit is synchronized in a laboratory and then transported to the test location. The temperature in the laboratory is similar to the test location but during transport the temperature is different. Now, frequencies in the laboratory and the testing site will be closer one each other because temperatures are the same in both locations. However, the phase and time error accumulates during transport. The longer the transport time and the temperature difference, the larger the error. The conclusion is that it is better to minimize the transport time when time and phase is to be tested because the accumulated error will be difficult to remove from the test result.

2.7.Using the Clock Reference Output

The Tempo clock reference output enables you to synchronize any external equipment with a clock signal generated by the tester or to connect the internal / recovered clock to an oscilloscope, spectrum analyser or other equipment. The reference clock output is therefore very useful for many tests related with network synchronization. These are the clock reference output ports and formats allowed by the test unit:

Table 2.14: PPS/ToD Reference Output Interfaces

Parameter	Description
Output ToD Protocol	Configures the protocol in a ToD clock reference output. The supported protocols are ITU-T G.8271 and NMEA. You can also disable the ToD protocol. In that case, the interface is equivalent to a 1 PPS over a balanced interface.
Output Reference delay	Adds a delay compensation to 1 PPS / 1PP2S / ToD clock reference output. This setting could be useful to configure the correct phase alignment at the output when the input is not able to compensate a phase offset.

- *Clock/PCM (REF IN/OUT)*: The clock reference output is encoded as a frequency or PCM signal. Options included in this set are 2048 kHz, E1,1544 kHz, T1, 5 MHz and 10 MHz. This signal is transmitted through the REF IN/OUT RJ-45 port. For this reason, this option is available only if a clock reference input has not been previously configured over the same port.
- *ToD (REF IN/OUT)*: Clock reference output constituted by a 1 PPS / ToD interface transmitted through the RJ-48 REF IN/OUT port. There are two ToD protocols supported: NMEA and ITU-T G.8271. This option is available only if a clock reference input has not been previously configured over the same port.

Table 2.15: IRIG-B Reference Output Interfaces

Parameter	Description
Modulation	Configures the IRIG-B signal modulation and encoding in a clock reference output. There are three possibilities: • A pulse width encoding (*Pulse width code (0)*) corresponding with the '0' identifier from the standard. • Amplitude modulated time code (*Sine-wave, AM (1)*) corresponding with the '1' identifier. • Manchester encoded signal (*Manchester modulated (2)*), which is identifier '2'. Amplitude modulated time codes are available only in unbalanced ports (SMB connector). Pulse width and Manchester time codes are available both over balanced and unbalanced ports.

Table 2.15: IRIG-B Reference Output Interfaces

Parameter	Description
Frequency	Configures the carrier frequency in modulated time codes. If the pulse width encoding is used then the only value for this parameter is *No carrier (0)*, which has identifier ‘0’ from the standard. For Manchester modulated signals, the carrier frequency is statically set to *1khz (2)*, corresponding to a 1 kHz modulation (identifier 2). Amplitude modulated codes accept a carrier frequency of 1 MHz (*1 MHz (5)*) which correspond with identifier 5.
Coded Expression	Describes the time code words used within the IRIG-B frame. It is a combination of encoded information providing details about time. Some of these encoded words are optional and one of them, the BCD Time-of-Year (*bcdtoy*), is mandatory. The optional codes are the *Straight Binary Seconds-of-day* (SBS), the *BCD Year* code, which encodes the current year, and the *Control Functions* (CF) that encode various control, identification or other special purpose functions.
Amplitude	Configures the signal amplitude in AM IRIG-B clock outputs. It could be either 8 V (peak-to-peak open circuit voltage) (*High*) or 4 V (peak-to-peak open circuit voltage) (*Low*).
Coupling	Configures the AC or DC coupling in AM IRIG-B outputs. AC coupling blocks any DC component form the line and DC coupling is transparent to all frequency components, including DC. In IRIG-B inputs, AC coupling is statically configured.
Impedance	Configures the output impedance in unbalanced PPS inputs. In unbalanced (SMB) outputs the impedance could be 50 Ω or 600 Ω.
Output reference delay	Configures the cable delay for the interface in nanoseconds. Keeping all delay sources under control in phase and time references is important to make sure that the signal significant instants are the same in all points in the network.

- *1 PPS (REF IN/OUT):* Generates a 1 PPS output synchronized (phase and frequency) with the local oscillator through the RJ-48 REF IN/OUT port. For this reason, this option is available only if a clock reference input has not been previously configured over the same port.
- *1 PP2S (REF IN/OUT)*: The clock reference constituted by a 1 PP2S signal (1 pulse every two seconds) transmitted through the RJ-48 REF IN/OUT port. For this reason, this option is available only if a clock reference input has not been previously configured over the same port.

- *1 PPS (REF OUT):* Generates a 1 PPS output synchronized (phase and frequency) with the local oscillator through the SMB REF OUT port.
- *1 PP2S (REF OUT)*: The clock reference constituted by a 1 PP2S signal (1 pulse every two seconds) transmitted through the SMB REF OUT port.
- *IRIG-B (REF IN/OUT)*: Generates an IRIG-B clock reference from any of the time codes available in the unit. The signal is transmitted through the RJ-48 REF IN/OUT port located in the test connector panel.
- *IRIG-B (REF OUT)*: Generates an IRIG-B clock reference from any of the time codes available in the unit. The signal is transmitted through the SMB REF OUT port located in the test connector panel.

Table 2.16: Clock/PCM Reference Output Interfaces

Parameter	Description
Clock/PCM input	Configures the Clock or PCM reference input interface: • *2048 kHz (Port Ref. In/Out)*: The clock reference is encoded as an unipolar, square wave 2048 kHz signal. This signal is transmitted through the balanced RJ-48 Ref. In / Out port. • *E1 (Port Ref. In/Out)*: The clock reference is encoded as an ITU-T G.703 2048 kb/s signal with an all ones-payload. This signal is transmitted through the balanced RJ-48 Ref. In / Out port. • *1544 kHz (Port Ref. In/Out)*: The clock reference is encoded as an unipolar, square wave 2048 kHz signal. This signal is transmitted through the balanced RJ-48 Ref. In / Out port. • *T1 (Port Ref. In/Out)*: is encoded as an ITU-T G.703 1544 kb/s signal with an all ones-payload. This signal is transmitted through the balanced RJ-48 Ref. In / Out port. • *5 MHz (Port Ref. In/Out)*: This is a 5 MHz unipolar, square wave 5 MHz clock transmitted through the RJ-48 Ref. In / Out port. • *10 MHz (Port Ref. In/Out)*: This is a 10 MHz unipolar, square wave 10 MHz clock output transmitted through the RJ-48 Ref. In / Out port.
Connector	Configures the port connector in a Clock / PCM reference input. Since all references of this type are currently transmitted through the balanced RJ-48 Ref. In / Out port, connector setting is not required.

Table 2.16: Clock/PCM Reference Output Interfaces

Parameter	Description
Frame structure	Sets the frame structure for E1 and T1 clock reference outputs. The available options are: • *PCM31*: 2048 kb/s TDM frame made up of 32 time slots (TS0, TS1,..., TS31) of 64 kb/s each. TS0 carries the FAS and NFAS words. All other time slots carry an all ones pattern. This frame structure is available only for E1 references. • *PCM31C*: 2048 kb/s TDM frame made up of 32 time slots (TS0, TS1,..., TS31) of 64 kb/s each. TS0 carries the FAS and NFAS words. The TS0 carries also a CRC-4 multiframe structure that enables error detection at the receiving end. All other time slots carry an all ones pattern. This frame structure is available only for E1 references. • *PCM30*: 2048 kb/s TDM frame made up of 32 time slots (TS0, TS1,..., TS31) of 64 kb/s each. TS0 carries the FAS and NFAS words. The TS16 carries the CAS multiframe that provides signalling to the user time slots. Time slots different of TS0 and TS16 carry an all ones pattern. This frame structure is available only for E1 references. • *PCM30C*: 2048 kb/s TDM frame made up of 32 time slots (TS0, TS1,..., TS31) of 64 kb/s each. This frame includes at the same time the *CRC-4* and *CAS* multiframes. Time slots different of TS0 and TS16 carry an all ones pattern. This frame structure is available only for E1 references. • *SF*: 1544 kb/s TDM frame made up of 193 bits and 24 time slots (TS0, TS1,..., TS23) of 64 kb/s each. The first bit in the frame defines a multiframe and carries an alignment sequence. Time slots from TS0 to TS23 of carry an all ones pattern. This frame structure is available only for T1 references. • *ESF*: 1544 kb/s TDM frame made up of 193 bits and 24 time slots (TS0, TS1,..., TS23) 64 kb/s each. The first bit in the frame defines a multiframe and carries different kinds of information including the alignment sequence, a data communications channel and a CRC-6 frame check sequence. Time slots from TS0 to TS23 of carry an all ones pattern. This frame structure is available only for T1 references.

Table 2.16: Clock/PCM Reference Output Interfaces

Parameter	Description
SSM signaling	Enables or disables the *Synchronization Status Message* (SSM) clock reference output. The SSM transports information about the current synchronization performance level transported in the E1 or T1 signal. The SSM information can be used by network clocks or other devices to know if the E1 or T1 signal is a reliable synchronization source. The SSM requires a frame structure with CRC in E1 interfaces (*PCM30C* or *PCM31C*). In T1 interfaces it requires FDL, which is only available with the ESF frame structure. The E1 NFAS also requires the user to configure which NFAS bit is used to transmit the message.

The configuration procedure to enable the reference clock output is detailed in the following steps:

1. From the *Home* panel, go to *CONFIG*,
   The port setup panel is displayed.
2. Go to *Reference clock*.
3. Configure Output clock to *Clock/PCM (REF IN/OUT)*, *ToD (REF IN/OUT)*, *1PPS (REF IN/OUT)*, *1PP2S (REF IN/OUT)*, *1PPS (REF OUT)*, *1PP2S (REF OUT)*, *IRIG-B (REF IN/OUT)*, *IRIG-B (REF OUT)*.
4. If you have chosen *Clock/PCM (REF IN/OUT)* in the previous step, configure *Clock/PCM Output, Connector, Frame structure and SSM signaling* from the *Clock/PCM output interfaces* menu.If you have chosen *ToD (REF IN/OUT)*, *1PPS (REF IN/OUT)*, *1PP2S (REF IN/OUT)*, *1PPS (REF OUT)* or *1PP2S (REF OUT)* configure the *Output reference delay* to compensate for the cable delay. If you have chosen *ToD (REF IN/OUT)*, configure the *Output ToD protocol* too. If you have configured *IRIG-B (REF IN/OUT)* or *IRIG-B (REF OUT)* configure the IRIG-B transmission parameters from the *IRIG-B output interfaces* menu.

Table 2.17: PPS/ToD output Interfaces Options

Parameter	Description
Output ToD Protocol	Configures the protocol in a ToD clock reference output. The supported protocols are ITU-T G.8271 and NMEA. You can also disable the ToD protocol. In that case, the interface is equivalent to a 1 PPS over a balanced interface.

Table 2.17: PPS/ToD output Interfaces Options

Parameter	Description
Output Reference delay	Adds a delay compensation to 1 PPS / 1PP2S / ToD clock reference output. This setting could be useful to configure the correct phase alignment at the output when the input is not able to compensate a phase offset. It could also be used for verification purposes.

Chapter 3
Cable Tests

Tempo has the ability to check wiring and performance of Ethernet cables or optical fibres to make sure they will operate as expected when connected to the network.

Cable testing can be used to estimate the cable length, recognise cabling types or detect wiring faults. Performance of optical fibers is measured in terms of the received optical power.

3.1. Electrical Test

Electrical cable test requires an special operation mode which prevents the unit sending any frame (See section 2.1). When the unit is configured in *Ethernet cable test*, mode, the port mode becomes *Cable test* (port A) and *Link* (port B) and there is no way to change the port mode unless the general operation mode is set to something different of *Ethernet cable test*.

In this operation mode the test unit could have a network link in the remote end of the device under test (the cable) or not. Depending on how the cable is connected, it would be possible to compute different results.

3.1.1. Basic Principles of Ethernet Cable Wiring

Twisted pair cables for Ethernet LAN applications generally come in groups of four pairs (8 wires). Only two of the four pairs carry information at 10 and 100 Mb/s but all four pairs are simultaneously used in 1 Gb/s links. There are many possible pair interconnections that would work, but only two of them are standard. These are known as T-568A and T-568B wire maps. Usually, all four pairs are always connected, but for 10 and 100 Mb/s operation only pairs 2 and 3 are used. 1 Gb/s port and cable wirings are designed to be backwards compatible with slower 10 Mb/s and 100 Mb/s interfaces so that the same Gigabit cable can be used for all bit rates. Some cables designed to operate at 10 Mb/s and 100 Mb/s may have only connections necessary for transmission at these speeds. These cables are not compatible with the 1 Gb/s bit rate.

Ethernet cables may have poor performance or may not work at all if wires are not properly connected.

All the different test results are provided for each *Media Dependent Interface* (MDI). An MDI corresponds with a single Ethernet pair transceiver. There are four of them in 1000BASE-T (MDI-0, MDI-1, MDI-2 and MDI-3) and two in 100BASE-TX / 10BASE-T (MDI-0 and MDI-1). Using the MDIs to supply information about wiring is the most logical choice: Pin assignment in a connector may change but MDIs are always the same and, at logical level, communication between MDIs is very simple: MDI-0 is connected to MDI-0, MDI-1 is connected with MDI-1, etc.

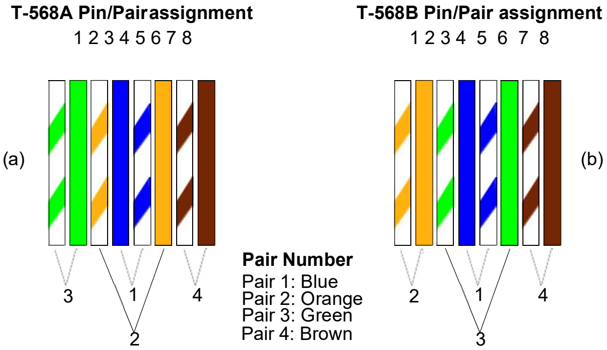


Figure 3.1: T-568A and T-568B wiring standards. Pair numbering (1, 2, 3, 4) is a way to identify pairs in the cable and is not to be confused with MDI numbering (MDI-0, MDI-1, MDI-2, MDI-3).

Old Ethernet stations had a fixed pin-out for MDI-0, MDI-1, MDI-2 and MDI-3. This fixed assignment for stations corresponds to the *MDI* status. These older stations were connected to Ethernet hubs and switches through a straight cable and to a second station through a crossover cable. For this reason, MDI pair assignment in hubs and switches was required to be complementary to the wiring of stations. This second pair assignment corresponds to the *MDIX* status:

Table 3.1: Pair assignment for MDI and MDIX port modes

	MDI-0	MDI-1	MDI-2	MDI-3
MDI	1-2	3-6	4-5	7-8
MDIX	3-6	1-2	7-8	4-5

In old devices with static MDI pair assignment, interface description could be based either on MDI-0 to MDI-3 or pair 1 to pair 8 but with most of the current Ethernet devices the situation is different. Modern Ethernet stations and switches can switch their ports between *MDI* and *MDIX* status before link establishment to make sure that an MDI port is connected with a remote MDIX port through an straight cable and that an MDI (or MDIX) port is connected to a second MDI (or MDIX) port through a crossover cable.

The advantage of this procedure is that there is no need to think about which cable (crossover or straight) is required for interconnection of network equipment and stations. However, if you need to know the way the cable is wired, then it is mandatory to know the MDI / MDIX status of the near and far ends.

Table 3.2: Crossover status (*MDI / MDIX*) and cable Wiring

Near end	Far end	Cable
MDI	MDI	Crossover
MDI	MDIX	Straight
MDIX	MDI	Straight
MDIX	MDIX	Crossover

3.1.2. Connecting the Tester

Cable testing with the *Ethernet cable test* mode is different to the other modes because in this case the test equipment does not generate any digital framed or unframed signal. It relies on the remote end to supply some information about the wiring and other metrics related with the physical transmission medium. The amount of information to be supplied depends on the communications interface. It is not the same for Gigabit Ethernet than for Fast Ethernet interfaces. If there is no link from the remote end, the equipment attempts to find out the reason (short circuit, open circuit...).

The cable test is available for Port A only. The Port B could be used as an auxiliary port to determine whether a cable is straight or crossover. Cable tests can only run from the native RJ-45 interfaces, they are not available through electric SFP modules.

The best way to run the cable test is to connect the cable under test between port A and port B. You can use other test configurations like a connection between Port A and a switch but in this case you will be unable to get all the information from the cable. Here you have some details about the available connection modes for the cable test and the results obtained from each of them:

- Port A - Port B closed loop: *Fault*, *Crosstalk*, *Distance (m.)*, *Crossover*, *Polarity*, *Skew (ns)*, *Wiring*.
- Port A connection with remote link: *Fault*, *Crosstalk*, *Distance (m.)*, *Crossover*, *Polarity*, *Skew (ns)*.
- Port A connection without link: *Fault*, *Crosstalk*, *Distance (m.)*.

In case a fault is found in some pair (*Open*, *Short*), some results may not be available for the corresponding MDI. If no fault is found then the *Distance (m)* field is empty. The *Skew (ns.)* test result is displayed only in 1000BASE-T interfaces.

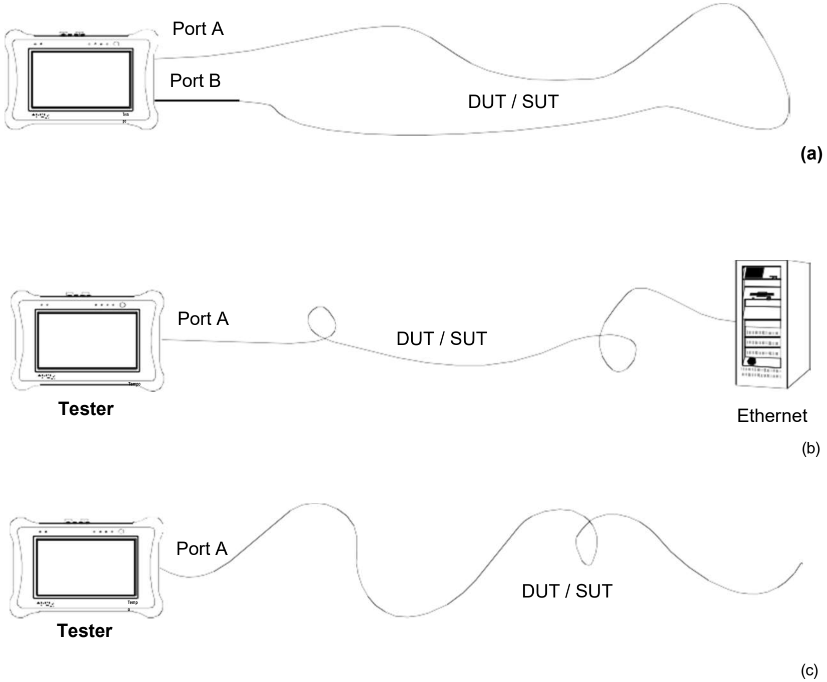


Figure 3.2: Basic connection setup for Tempo tester: (a) Port A - Port B closed loop, (b) Port A connection with remote link, (c) Port A connection without link.

3.1.3. Running the Test

Once the tester has been connected to the network in any of the supported test configurations. It is required to configure and run the cable test by means the tester user interface. It is assumed that the *Connector* setting is configured to *Electrical* in the test ports (See section 2.2.1). The test procedure is as follows:

1. From the *Home* panel, go to *CONFIG*,
   The port setup panel is displayed.
2. Select *Mode* to enter in the mode selection menu

3. Choose *Ethernet cable test*.
4. From the *Home* panel, go to *Results*,
   The port setup panel is displayed.
5. Select *Port A* to enter in the test Port A specific results panel.

Table 3.3: Common cable wiring problems

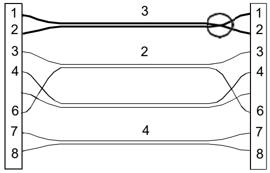
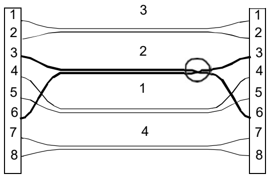
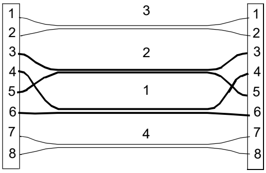
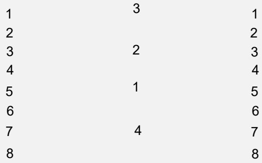
Description	Diagram	Diagnostic
Inverted cable. Polarity is inverted in both ends of the same pair	 1 2 3 4 6 7 8 3 2 4 1 2 3 4 6 7 8	The *Polarity* result for de corresponding MDI (MDI-0, MDI-1, MDI-2 or MDI-3) is *Negative* rather than *Positive.*
Pairs 1 and 2 are wired to the wrong pins in the connector	1 2 3 4 5 6 7 8 3 2 1 4 1 2 3 4 5 6 7 8	The *Fault* result for MDIs corresponding to pairs 1 and 2 is *Open*. *Distance (m)* displays the distance to the far end. The *Crosstalk* shows that pairs 1 and 2 are coupled.
There is a short circuit between the conductors in pair 2	 1 2 3 4 5 6 7 8 3 2 1 4 1 2 3 4 5 6 7 8	The *Fault* result for the MDI corresponding to pair 2 displays *Short*. *Distance (m)* displays the distance to the short circuit.
One of the cables of port A is broken and it contains an open circuit	1 2 3 4 5 6 7 8 3 2 1 4 1 2 3 4 5 6 7 8	The *Fault* result for the MDI corresponding to pair 2 displays *Open*. *Distance (m)* displays the distance to the open circuit.

Table 3.3: Common cable wiring problems

Description	Diagram	Diagnostic
Swapped pair, connections are OK but wires of the same connection are twisted in different pairs.		No fault is detected in any pair (*Fault* displays *OK* for all MDIs) but if the cable is long enough it will result in large crosstalk between coupled pairs.
Miswired cable		The diagnostic of the cable shows crosstalk between the MDIs corresponding to pairs 2 and 3.

6. Go to Cable
   The Ethernet cable test result panel is displayed
7. Run the test by pressing the *Run* button and wait a few seconds to the end of the measurement.
8. Check the *Fault*, *Crosstalk*, *Distance (m.)*, *Crossover*, *Polarity*, *Skew (ns.)* and *Wiring* test results for each MDI-*n*.

Table 3.4: Cable test results

Result	Description
Fault	Displays information about faults found inthe corresponding MDI. In case a fault is found the *Fault* indication could be either *Open* or *Short*. • *Open* means that it has been found an open circuit in the remote end. An open circuit is declared when the impedance in the remote end is very large (the reflection coefficient is close to 1). • *Short* means that it has been found a short circuit in the remote end. The short circuit is declared ifthe impedance in the remote end is zero or close to zero (the reflection coefficient is close to -1).

Table 3.4: Cable test results

Result	Description
Crosstalk	Crosstalk is detected when there is electromagnetic coupling between pairs. Coupling could be inductive / capacitive if there is a twisting defect in the pair or it can be resistive if there is a problem with the dielectric medium between conductors. Some wiring faults between the cable and the connector may cause crosstalk too. The crosstalk is indicated in the equipment as a collection of numbers separated by '-' for each MDI. For example if MDI-0 and MDI-3 are coupled, then the crosstalk result for MDI-0 and MDI-3 will be 0-3.
Distance (m.)	The *Distance (m.)* result displays the distance to an open circuit / short circuit fault in with an accuracy of ±1 m. If there is no fault, no distance is displayed. The maximum range of the distance test is 100 m. To measure the cable length, just leave the far end disconnected and run the test. Tempo will detect an open circuit in all MDIs and the *Distance (m.)* results displays the cable length.
Crossover	Displays whether the local *MDI-n* is in straight (MDI) or crossover (MDIX) status. Note that *Crossover* is not really a cable result, it is the local port MDI/MDIX status. This status may be random and depends on the cable and the remote port. Therefore this result may be modified if the cable is disconnected and reconnected again.
Polarity	Polarity could be positive or negative for each *MDI-n.* A negative polarity indicates that the pair connects pins of inverted polarity in the local and remote end. Positive polarity means that local and remote pins have the same assigned polarity.
Skew (ns.)	Relative propagation delay, expressed in nanoseconds, experienced by the pair associated to the MDI and compared to the MDI that has minimum propagation delay. That means that the Skew (ns.) is always zero for at least one MDI. The skew result is not measured for 10 Mb/s and 100 Mb/s interfaces.

Table 3.4: Cable test results

Result	Description
Wiring	A cable could be designed to cross at the remote end the pairs used for transmitting and receiving (crossover cable) or not (straight cable). The wiring result checks whether a cable is straight or crossover. This test result depends on the local and remote MDI / MDIX status and it can only be determined if the cable is connected through test port A and B.

3.2. Measuring Optical Power

The test unit reports the transmitted and received optical power if it is equipped with SFP / SFP+ supporting this measurement (See section 2.2.2). The following description assumes that the *Connector* setting is configured to *Optical* in the test ports (See section 2.2.1). The test procedure is as follows:

1. From the *Home* panel, go to *CONFIG*,
   The port configuration panel is displayed.
2. Select *Mode* to enter in the mode selection menu
3. Choose *Ethernet endpoint, IP endpoint or IP through*.
4. From the *Home* panel, go to *RESULTS*,
   The port setup panel is displayed.
5. Select either *Port A or Port B* to enter in the port specific results menu.
6. Go to *SFP information*.
7. Check the results of *TX optical power* and *RX optical power.*

3.3. Measuring PoE / PoE+ Electrical Parameters

Power over Ethernet (PoE) is a technology that enables remote powering of devices such as VoIP telephones or cameras through the electrical Ethernet interface, commonly based in CAT 5 or CAT 6 UTP cable, so that these devices do not need any other external power source.

PoE was defined in standard IEEE 8023af in 2003 and was improved in 2009 in the standard IEEE 802.3at, known as PoE+. The first version of the standard was designed to provide powers up to 15.4 W but IEEE 802.3at supports up to 25 W. Some current commercial PoE+ devices can deliver much higher powers, however.

The PoE / PoE+ standard defines two devices, the Power Source Equipment (PSE) and the Powered Device (PD). The PSE generates the power required to feed the PD and it can be an *Endspan* or a *Midspan*. Endspans are usually Ethernet switches or routers with PoE / PoE+ functionality. On the other hand, Midspans are devices connected between a switch or a router without PoE / PoE+ and the PD. These Midspans inject the current required to feed the PD.

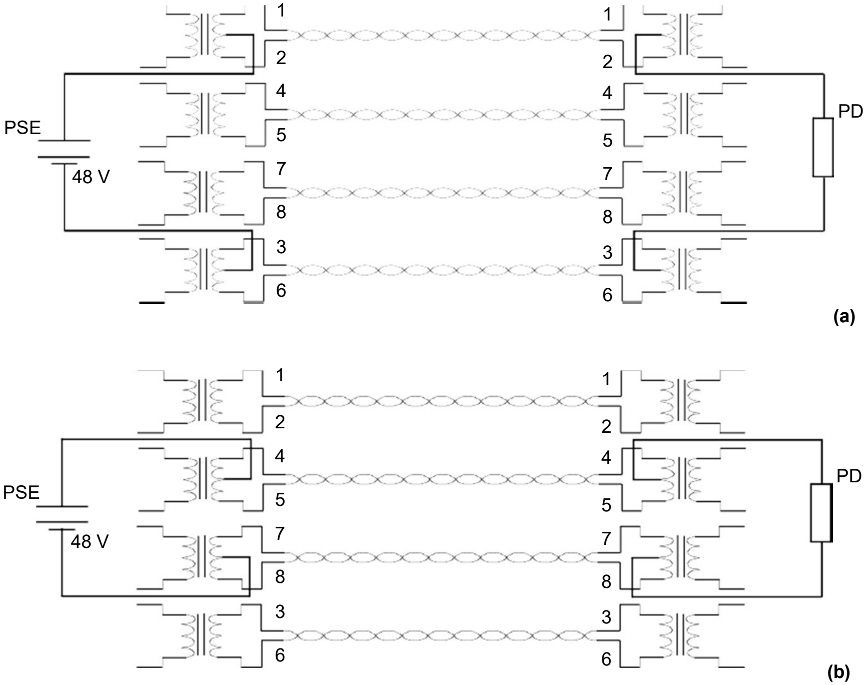


Figure 3.3: PoE / PoE+ powering alternatives: (a) Alternative A, power is injected between wires 1/2 and 3/6. (b) Alternative B, power is injected between wires 4/5 and 7/8.

To deliver power to the PD, the PoE / PoE+ standards define to different options. The alternative A injects power between wires 1/2 and 3/6 while the Alternative B uses pairs 4/5 and 7/8 to deliver power. The PoE / PoE+ implements a simple protocol to avoid injecting power in non-PoE devices. Before injecting a large amount of current in the line, the PSE senses the PD to see how much current it consumes. Once the PD identification has finished the PSE increases the voltage and classifies the PD depending on the consumed current in five categories numbered from 0 to 4. Finally the PSE stabilizes the voltage to around 48 V DC and the normal powering operation starts.

Table 3.5: Cable test results

Result	Description
Status	Displays the current PoE / PoE+ measurement status. The *Status* could be any of the following items: • *Measuring*: The system has detected PoE or PoE+ andit is measuring normally. • *No PoE*: No PoE / PoE+ detected. No test result isdisplayed. • *Error*: Unspecified error condition. It should neverappear in normal circumstances.
Voltage	Displays the voltage measured between wires 1/2 and 3/6 (Alternative A). This result is available both in endpoint and pass-through modes.
Polarity alternative A	If the current powering alternative is Alternative A, it displays which of the 1/2 or 7/8 wires has positive and negative polarity. If the power alternative is Alternative B, it displays no result.
Current	If the powering alternative is Alternative A, it displays the current injected in the PD.If the power alternative is Alternative B, it displays no result. This result is available only in the equipment is connected between the PD and PSE in pass-through mode.
Power	If the powering alternative is Alternative A, it displays the power injected in the PD. If the power alternative is Alternative B, it displays no result. This result is available only in the equipment is connected between the PD and PSE in pass-through mode.
Polarity alternative B	Displays the voltage measured between wires 4/5 and 7/8 (Alternative B). This result is available both in endpointand pass-through modes.
Current	Displays the Alternative B current in the same conditions that the Alternative A
Power	Displays the Alternative B power in the same conditions that the Alternative A current

Tempo may optionally include support for PoE and PoE+ measurement. The unit is compatible both endpoint and pass-through measurements. If the tester is connected in endpoint mode, it replaces the PD and it is capable of measuring the PoE / PoE+ voltage as generated by the PSE. In pass-through mode, the measurement includes voltage, current and power. The correct test procedure is as follows:

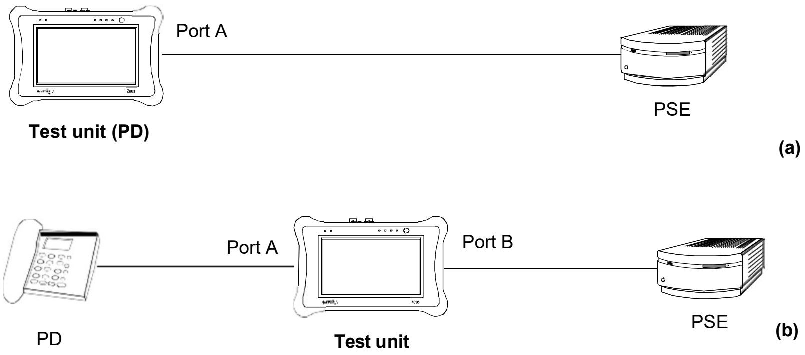


Figure 3.4: Connection of Tempo to measure PoE / PoE+: (1) The test unit replaces the PD. The unit measures only voltage, (2) The test unit is connected between the PD and the PSE, In this case it measures voltage, current and power.

1. Connect the equipment either in endpoint or pass-through mode (See section 2.2).
1. From the *Home* panel, go to *CONFIG*,
   The port configuration panel is displayed.
2. Select *Mode* to enter in the mode selection menu
3. Choose *Ethernet endpoint, IP endpoint or IP through*.
4. Go to *Port A.*
   The port specific settings for Port A are now displayed.
5. Go to *Physical layer* to enter in the physical settings configuration panel.
6. Configure the *PoE* setting to *On*.

Once configured, you can check the test results by following these steps:

1. From the *Home* panel, go to *CONFIG*,
   The port configuration panel is displayed.
2. Go to *Port A.*
   The port specific settings for Port A are now displayed.
3. Select the PoE results menu and make sure that the status is *Measuring*.
4. Check the Voltage result in endpoint mode or *Voltage* and *Polarity*, *Current* and *Power* for your PoE / PoE+ alternative in pass-through mode.

Chapter 4
Traffic Generation

One of the key features of Calnex family of Ethernet Generators & Analysers is the ability to generate traffic with deterministic and random bandwidth profiles. The traffic generation feature can be used to stress the network, simulate user traffic and, if a suitable payload is configured, to measure critical network performance parameters like bit errors, packet loss or latency.

Tempo has eight independent full featured traffic generators attached to each of the available Ethernet / IP test ports (*Port A* and *Port B*). Each traffic flow may be configured with specific encapsulation and addressing parameters thus providing great versatility in all applications requiring Ethernet and IP traffic generation.

4.1. Generation of Ethernet Traffic

In the test unit, generation of custom Ethernet frames is available for Port A in *Ethernet endpoint* mode through the *Frame*, *Bandwidth profile* and *Payload* settings for each of the eight available traffic flows. This is a short description of the Ethernet traffic generation menus:

- *Frame*: Configures the encapsulation and MAC addresses. If the Ethernet frames have any VLAN tag, this menu configures the VID and priority for these tags.
- *Bandwidth profile*: Sets the traffic generation statistics. There are four different generation profiles to choose: *Constant*, *Periodic burst*, *Ramp* and *Random*.
- *Payload*: This menu is used to set the payload to be inserted in the generated Ethernet frames. The SLA payload enables the user to measure delay, jitter and packet loss. The BERT payload (flow 1 only) is used for BER testing in framed interfaces.

Frame generation capability is controlled by the *run* button. That means that no test traffic is generated if you don't press *run*. However, the tester may generate signalling traffic or reply to certain messages like ARP or ICMP echo requests even if there is not an ongoing test. Some automatic tests like the RFC 2544 or the eSAM have their own internal traffic generation dynamics but they are controlled by the RUN button as well.

4.1.1. Physical Layer Settings

Before starting any frame generation test, the equipment must be connected to the network and the electrical and optical physical layer must be correctly configured. Ethernet technology has been designed to keep physical layer configuration to the minimum. But there are at least two settings you may need to check before you get a link from the DUT / SUT. These settings are the *Connector* (See section 2.2.1) and the *Auto-negotiation* (See section 2.2.3). You will know that the port is prepared for traffic generation and analysis when the *10G, 1000, 100* or *10* LED (See section 5.3) is displayed in green colour.

4.1.2. Frame Settings

Most of the Ethernet frame fields are available for configuration in the test unit. Before configuring these fields it is necessary to tell to the tester which frame structure is going to be used for traffic generation. The *Frame type* is a port-wide setting. Once you choose an specific framing for your traffic, all streams you define for the port carry the same framing structure. The only currently available *Frame type* is *DIX*, The *DEC, Intel, Xerox* (DIX) frame, structure also known as Ethernet II framing. DIX / Ethernet II framing encode the payload type in the *Type* frame field. This is the most common framing format found in real networks: For example, RFC 894 mandates a DIX / Ethernet II frame structure with the *Type* field set to 0x0800 for IPv4 encapsulation.

Table 4.1: Ethernet Frame Settings

Setting	Description
Encapsulation	This field configures the way the data is encapsulated in Ethernet frames for transmission in the current stream.The allowed encapsulations are the following ones: • *None*: A DIX or IEEE 802.3 frame carries the test data, depending on the current value of the *Frame type* setting. • *VLAN*: Transmitted frames are labelled with an IEEE 802.1Q frame tag. Settings related with configuration of the VLAN tag are enabled when this option is selected. • *Q-in-Q*: Transmitted frames carry two VLAN tags, one service provider tag (S-VLAN) and a customer tag (C-VLAN). The C-VLAN is identified by the normal IEEE 802.1Q Ethertype and the S-VLAN carries one of the not-standard Ethertypes. • *IEEE 802.1ad*: Transmitted frames carry two VLAN tags. It is similar to the Q-in-Q encapsulation but this option follows strictly the standard IEEE 802.1ad encapsulation for Provider Bridges (PB). Specifically, the IEEE 802.1ad carries the special 0x88a8 Ethertype within the S-VLAN.

Table 4.1: Ethernet Frame Settings

Setting	Description
Encapsulation	• *Local Profile*: Sets the encapsulation (and eventually the C-VID and C-VLAN priority) to the same value configured in the local profile (See section 2.3). This is the default configuration. It is useful when the user wants to control the encapsulation in various streams through a single setting.
Source MAC address from	Establishes the origin of the source MAC address for the current stream. There are two possible settings: • *Local*: The source address is set to the factory MAC address assigned to the port. Use this setting if there is no other requirement. • *Manual*: The source address is set to the value configured in *Source MAC address*. Use manual MAC addresses if you want to simulate traffic generated by an equipment different to the tester or, in multi-stream operation, to simulate traffic transmitted from different stations. Most of the times you will want to avoid duplicated addresses in your network. For this reason, make sure that no other equipment is using the manually configured MAC address. • *Remote*: This option is available only in RFC 2544 or eSAM downstream asymmetric tests (See section 7.4). It configures the source MAC address to be the far end address. It must be taken into account that in downstream asymmetric tests, the far end is configured for traffic generation this setting corresponds with traffic to be generated not in the local unit but in a different one.
Source MAC address	Source MAC address carried by the frames generated in the current stream if *Source MAC address type* is set to *Manual*. Anything from 00:00:00:00:00:00 to ff:ff:ff:ff:ff:ff is allowed.

Table 4.1: Ethernet Frame Settings

Setting	Description
Des. MAC address from	Establishes the origin of the destination MAC address for the current stream. There are three different settings available for configuration: • *ARP*: Uses the Address Resolution Protocol (IETF RFC 826) to configure the destination MAC address without user intervention. The ARP requires the IPv4 destination address to be previously configured to work. For this reason, ARP is available only in *IPendpoint* mode. • *Manual*: The destination address is set to the value configured in *Destination MAC address*. • *Range*: Test data in the current stream is transmitted to a group of MAC addresses configured with *Destination MAC address* and *Address number within range*. Use this option if you want to deliver the test data sequentially to many different destinations. • *Port A / Port B*: Configures the opposite port in the same unit as the destination for the traffic. Port B is displayed as one of the accepted destinations for Port A and Port A is shown in Port B with the same purpose. • *Remote*: This option is available only in RFC 2544 or eSAM upstream asymmetric tests (See section 7.4). It configures the destination MAC address to be the far end address.
Destination MAC address	Destination MAC address carried by the frames generated in the current stream if *Des. MAC address type* is set to *Manual*. If *Des. MAC address type* is set to *Range*, this field contains the first destination MAC address within the range. Anything from 00:00:00:00:00:00 to ff:ff:ff:ff:ff:ff is allowed for this field.

Table 4.1: Ethernet Frame Settings

Setting	Description
Address range size	Configures the number of MAC addresses within an address range. This control is valid only if *Des. MAC address type* is set to *Range*. In this case, the Ethernet frames transmitted in the current stream will contain as many destination addresses as previously configured in this field. The destination MAC address is increased by one unit for each transmitted frame starting with the value configured in *Destination MAC address*. If there are no more addresses left in the range, transmission returns to the initial address and starts the process from the beginning.
Ethertype	Ethertype value carried by the frames generated in the current stream. This value is found within the Ethernet *Type* header field in DIX / Ethernet II frames or within the LLC / SNAP header in IEEE 802.3 frames. Depending on the configuration, the *Ethertype* value is fixed and cannot be set by the user. If the operation mode is *IP endpoint*, the Ethertype is automatically configured to 0x0800 (Internet Protocol, version 4). If the payload type is configured to *SLA* in *Ethernet endpoint* mode, the Ethertype is set to 0x8902 (IEEE 802.1ag / ITU-T Y.1731 OAM) to account for the special structure of the Ethernet SLA measurement payload (See section 4.1.3, however).
C-VID	VLAN identifier assigned to tagged frames (IEEE 802.1Q) or C-VLAN identifier for double tagged frames (IEEE 802.1ad, Q-in-Q). In frames with two VLAN tags, the C-VID usually accounts for the VLAN structure corresponding to the customer network. Any value within 0 to 4095 is allowed for this field.
C-VLAN priority	3-bit class of service (CoS) field defined to set frame groups with different priorities or to provide specific treatments to special frames within a network or an administrative domain. This field is carried by the Q-tag of Ethernet frames with a single tag or by the C-tag of Ethernet frames with two tags. Any value from 0 to 7 is allowed for this field. Specific actions to be carried out on frames with different CoS labels depend on the network and the service provider.

Table 4.1: Ethernet Frame Settings

Setting	Description
S-VLAN TPID	Ethertype to be associated to the S-VLAN tag in Q-in-Q frames. Four different values are possible: 0x8100, 0x9100, 0x9200 and 0x9300. It the encapsulation is set to IEEE 802.1ad, the S-VLAN Ethertype is automatically set to 0x88a8 and this field is not available for configuration.
S-VID	VLAN identifier assigned to the S-tag in double tagged frames (IEEE 802.1ad, Q-in-Q). In frames with two VLAN tags, the S-VID usually accounts for the VLAN structure corresponding to the service provider network. Any value within 0 to 4095 is allowed for this field.
S-VLAN priority	3-bit class of service (CoS) field defined to set frame groups with different priorities or to provide specific treatments to special frames within a network or an administrative domain. This field is carried by the S-tag (service provider tag) of Ethernet frames with two tags. Any value from 0 to 7 is allowed for this field. Specific actions to be carried out on frames with different CoS labels depend on the network and the service provider.
Drop-eligible indicator	This is a single bit field that is used to mark drop eligible frames. These frames are usually dropped first when congestion is detected in a network node. The Drop eligible operator is carried within the S-tag of IEEE 802.1ad frames.
Frame size	Ethernet MAC frame size including the destination MAC address, source MAC address, type / length field, payload, FCS and any VLAN tag carried by the frame. Anything between 64 B and 10000 B is allowed but frames longer than 1518 B (without VLAN tags and MPLS labels) are out of the IEEE 802.3 standard. It is possible to generate frames longer than the port Maximum Transmission Unit (MTU) but these frames are considered oversized frames when they are analysed by the tester. To avoid an *OverS* anomaly in this case, increase the value of the port MTU.

The second port-wide setting to be configured is the Maximum Transmission Unit (MTU). This setting is relevant for the analyser only and it configures the largest frame size accepted without declaring the *OverS* defect. Standard IEEE 802.3 specifies an MTU of 1518 bytes for ordinary Ethernet frames but 1522 is admitted for VLAN frames and 1526 is valid for frames carrying two VLAN tags (IEEE 802.3ad, Q-in-Q). Some switches provide support for much larger frames known as jumbo frames. These frames are more efficient because the ratio of header bytes to payload bytes is smaller for larger frames but they are currently not accepted by any international standard.

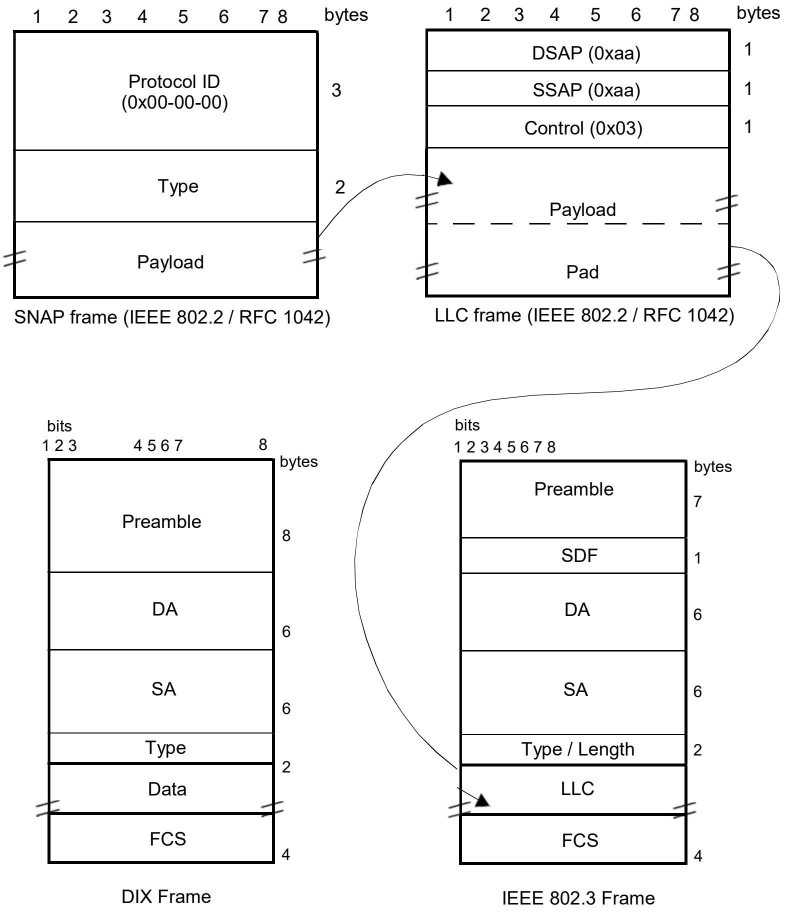


Figure 4.1: MAC frame structure: IEEE 802.3 and DIX

The following steps illustrate the frame configuration procedure in Tempo. Both the port-wide and flow-specific configuration is included.

1. Make sure that your tester is connected to the network. The physical layer must be up and working (See section 4.1.1).
2. From the *Home* panel, go to *CONFIG*,
   The test port settings panel is displayed.
3. Select either Port A or Port B to enter in the port specific configuration.
4. Enter in the *Frame* menu.
   All settings related with frame configuration are displayed.

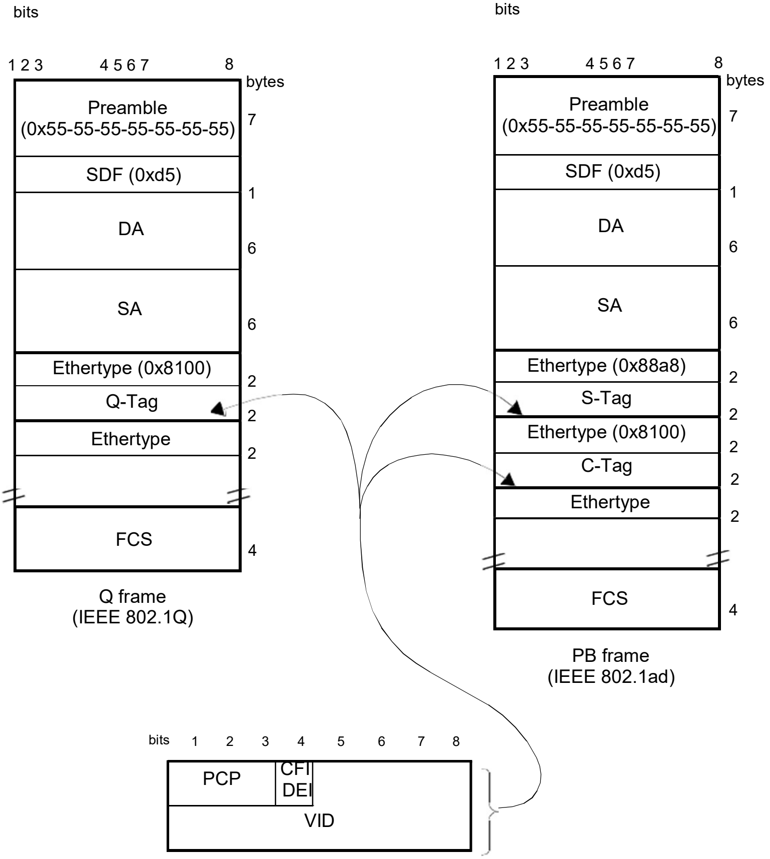


Figure 4.2: IEEE 802.1Q y IEEE 820.1ad frame structures.

5. Configure the correct MTU with the help of the *MTU* menu. You may want to set the MTU to 1518 bytes for traffic analysis in line with IEEE 802.3 or to other value to allow jumbo frames. The maximum allowed MTU is 10,000 bytes.
6. Select one of the traffic flows between *Flow A1* and *Flow A8* (or *Flow B1* to *Flow B8* in *Port B*) to enter in the flow specific configuration.
7. Configure the encapsulation you are going to use in the generated frames. Basically, the *Encapsulation* menu sets the number of VLAN tags to be included in the generated frames.
8. Enter the source MAC address with the help of the *Source MAC address from* and *Source MAC address* controls. You can configure the factory MAC address as the source address for the generated frames or enter a custom address.
9. Enter the destination MAC address or addresses by using the *Destination MAC address from*, *Destination MAC address* and *Address range size*. If you choose to generate a destination address range you will be requested to enter the number of addresses that made up the range.
10. Configure the *Ethertype* value.
    Note: Some frame structures require an specific value of the Ethertype. This field cannot be configured in this case.
11. If you are using frames carrying one (IEEE 802.1Q) or two (IEEE 802.1ad, Q-in-Q) VLAN tags, enter the *C-VID* and *C-VLAN priority*.
12. If you are using frames carrying two VLAN tags (IEEE 802.1ad, Q-in-Q), enter the *S-VID*, *S-VLAN priority* and *Drop-Eligible Indicator*.
13. If you are generating not-standard Q-in-Q frames, set the *S-VLAN TPID* to one of the allowed values.
14. Configure the frame length to the correct value with the help of *Frame size*.
15. If necessary, repeat the specific flow configuration for one or more traffic flows (*Flow B1* to *Flow B8* or *Flow B1* to *Flow B8*, depending on the test port) from the *Frame* menu.

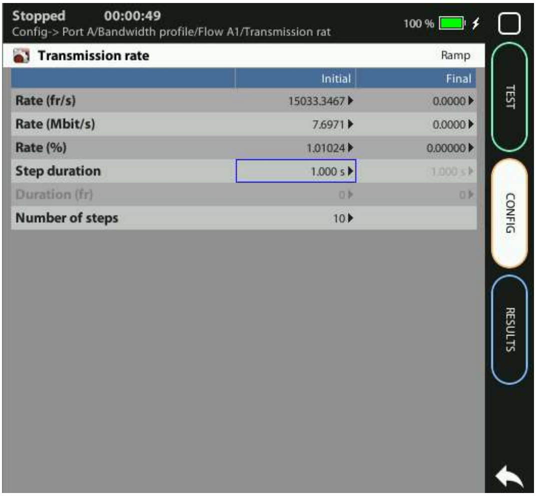
4.1.3. Configuring the Bandwith Profile

In the same way that the *Frame* menu configures the frame format for each of the available traffic flows, the *Bandwidth profile* sets how many frames are transmitted and how transmission events are distributed in time. The simplest is to generate frames with a constant bit rate specified in frames per second, bits per second or as a percentage of the total transmission channel capacity. However, the test unit provides other alternatives to the constant transmission like the periodic burst, ramp transmission or random transmission with Poisson statistics.

The bandwidth profile settings are available only in port Port A because the traffic generator is not available in Port B. The procedure to configure the bandwidth profile in a traffic flow is as follows:

1. Make sure that your tester is connected to the network. The physical layer must be up and working (See section 4.1.1).

2. From the *Home* panel, go to *CONFIG*,
   The test port settings panel is displayed.
3. Select Port A or Port B to enter in the port specific configuration.
4. Enter in the *Bandwidth profile* menu.
5. Select one of the traffic flows between *Flow #1* and *Flow #8* to enter in the flow specific configuration.
   All configuration items related with the bandwidth profile are displayed.
6. Configure the transmission mode to one of the available profiles with the help of the *Mode* control.



Stopped 00:00:49

Config-> Port A/Bandwidth profile/Flow A1/Transmission rat

Transmission rate Ramp

	Initial	Final
Rate (fr/s)	15033.3467 ▸	0.0000 ▸
Rate (Mbit/s)	7.6971 ▸	0.0000 ▸
Rate (%)	1.01024 ▸	0.00000 ▸
Step duration	1.000 s ▸	1.000 s ▸
Duration (fr)	0 ▸	0 ▸
Number of steps	10 ▸	

Figure 4.3: Calnex Tempo bandwidth profile configuration panel.

7. Configure the transmission rate parameters with *Transmission Rate*.
   Note: Depending on the current transmission mode you will be requested to enter different traffic parameters in the *Transmission Rate* panel.
   Note: Changing some transmission parameter may affect the value of other parameters previously configured in the same panel. For example, setting the transmission rate in frames per second modifies the rate in bits per second and the percentage value of the transmission rate.
   Note: If the channel capacity varies, the transmission rates configured as percentages of the overall channel capacity are kept to the same value but the bits per second and frames per second are recomputed for the new channel capacity.

8. If necessary, repeat the bandwidth profile configuration process for one or more traffic flows (*Flow #1* to *Flow #8*) available from the *Bandwidthprofile* menu.

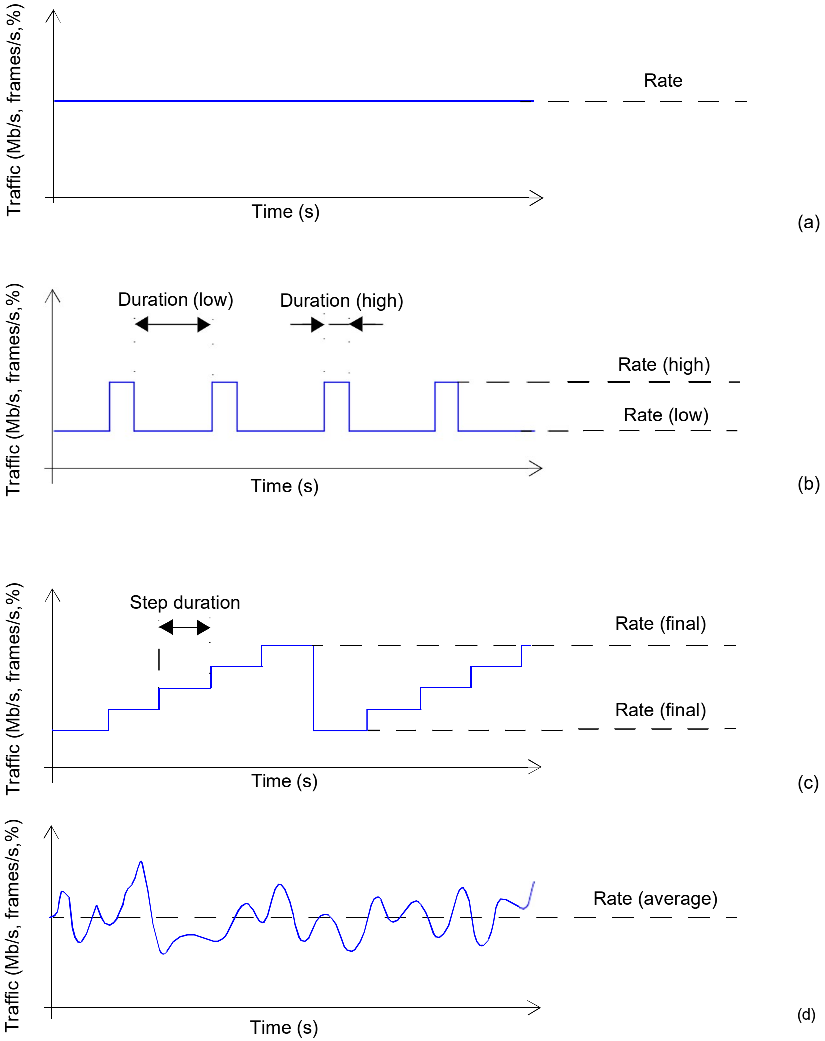


Figure 4.4: Bandwidth profiles forCalnex Tempo: (a) Continuous traffic generation, (b) Periodic burst generation, (c) Ramp generation, (d) Random traffic generation with Poisson probability distribution.

Test traffic generation does not start immediately after setting the bandwidth profile parameters. Traffic generation requires a test to be started with by pressing *run*.

Table 4.2: Ethernet Payload Settings

Setting	Description
Mode	Configures the traffic shape to be used by the traffic generator in the current stream. There are five possible generation modes for this for the bandwidth profile • *Off*: No frames are transmitted in the current stream. Use this setting if you want to disable traffic generation in the current stream but you don’t want to globally disable generation in the test port. • *Continuous*: Frames is transmitted at a constant speed to match a value configured in bits per second, frames per second or a percentage of the line capacity. • *Periodic burst*: Traffic generation is distributed in periodic bursts of fixed length. Between traffic bursts the user may choose to generate background traffic or disable traffic generation. • *Ramp*: Generates traffic that increases its bit rate with time in steps. The number of steps and step duration are configured by the user. Minimum and maximum traffic generated in the ramp are user configurable as well. Ramp generation is periodic. Traffic generator is restarted when it finishes with the last step of an specific ramp. • *Random*: The number of frames generated per time unit is a Poisson random variable. This is equivalent to say that the distance between two consecutively generated frames is an exponential random variable. Use the Random generation profile to generate traffic that resembles network traffic as much as possible.

Table 4.2: Ethernet Payload Settings

Setting	Description
Transmission rate	This control displays an editable table that enables the user to enter the parameters associated with the traffic to be generated by the current stream. Parameters to be configured depend on the current bandwidth profile generation mode: • *Continuous* traffic: The relevant bandwidth parameter is the transmission *Rate* configured in *fr/s*, *Mb/s* or *percentage*. • *Periodic burst*: Values to be entered are the high and low transmission rates (in *fr/s*, *Mb/s* or *percentage*) and the high and low durations expressed in seconds or frames. • *Ramp*: Relevant configuration parameters are the initial and final transmission rates (in *fr/s*, *Mb/s* or *percentage*), the *Step duration* configured in seconds and the *Number of steps*. • *Random*: The bandwidth parameter to be configured is the average transmission rate in *fr/s*, *Mb/s* or *percentage*.

4.1.4. Choosing the Test Payload for Ethernet

The traffic generated by Tempo is synthetic. It does not contain any real user data. In fact, the user payload of the internally generated frames is replaced by a test payload. Many times, test payloads are much more than dummy bit sequences designed to replace the user traffic. Test payloads may contain time stamps or sequence numbers that determine which test metrics are available from the result panels or which tests will be run. For this reason, configuration of the right test payload is important to get the required results.

Selection of the test pattern is relevant both for the generator and the analyser. When you generate a test payload or pattern in Port A, the same port is automatically configured so that it is waiting for frames carrying the same pattern in the receiver. Settings related with test payload / pattern selection are available both in Port A and Port B. The procedure to select the test payload in the tester is as follows:

1. Make sure that your tester is connected to the network. The physical layer must be up and working (See section 4.1.1).
2. From the *Home* panel, go to *CONFIG*,
   The test port settings panel is displayed.
3. Select either *Port A* or *Port B* to enter in the port specific configuration.
4. Enter in the *Payload* menu.
5. Optionally, if you need to generate the SLA payload, configure a custom Ethertype value by setting *SLA EtherType from* to *Manual* and then entering the Ethertype in *SLA EtherType value*,

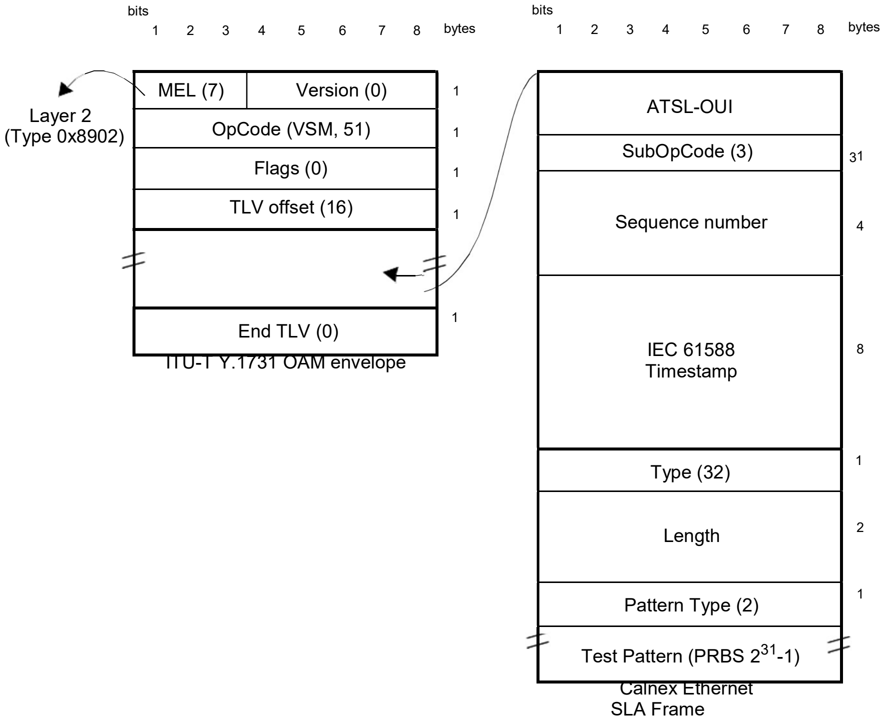


Figure 4.5: Calnex payload for SLA tests (Ethernet Endpoint mode).

Note: The default value for the SLA Ethertype in *Ethernet endpoint* mode is 0x8902 (IEEE 802.1ag / ITU-T Y.1731 OAM). There is no way to set a custom Ethertype in IP endpoint mode, which is statically set to 0x0800 (IPv4 protocol).

6. Select one of the traffic flows between *Flow 1* and *Flow 8* to enter in the flow specific configuration.
   All settings related with payload configuration in the current flow are displayed.
7. Choose one of *BERT*, *SLA* or *All zeroes* in *Payload type*.
   Note: BER is available only for flow 1.
8. If you have configured *Payload type* to BER, choose the bit pattern you are going to use for generation and analysis with the help of the *BERT patterns*control.
9. If you have configured *BERT patterns* to *User*, enter a 32-bit test pattern in *User payload* in hexadecimal format.

10. If necessary, repeat the payload configuration process for one or more traffic flows (*Flow #1* to *Flow #8*) available from the *Payload* menu.

Table 4.3: Ethernet Frame Settings

Setting	Description
Payload Type	• *BERT:* The payload content is set to a bit pattern suitable for measuring the Bit Error Ratio (BER). The tester includes support for two different kinds of BERT pattern: Pseudo-Random Bit Sequences (PRBSs) or 32-bit user configurable patterns. BERT generation and analysis over framed interfaces is supported by flow 1 only. • *SLA:* This is the payload to be used to measure latency, packet loss and all the SLA metrics derived from them. If the current operation mode is set to *Ethernet endpoint*, the SLA payload constitutes a proprietary extension of the Operation, Administration and Maintenance (OAM) protocol for Ethernet defined in ITU-T Y.1531. The SLA payload in *IP Endpoint mode* is a proprietary Calnex format. • *All zeroes*: Sets the transmitted pattern to all zeroes.
BERT Patterns	Sets the transmitted and expected test pattern (port A) or the expected test pattern (port B). Supported patterns are: • *PRBS 2^{11}-1 /2^{11}-1 inverted*: This is a pseudo-random bit pattern specified in ITU-T O.150 and O.153 for error performance measurements below the primary rate (2048 kb/s). The 2^{11}-1 inverted is a 2^{11}-1 bit wise inverted pattern. • *PRBS 2^{15}-1 /2^{15}-1 inverted*: This is a pseudo-random bit pattern specified in ITU-T O.150 and O.151 for measurements at the primary rate or above. The 2^{15}-1 inverted is a 2^{15}-1 bit wise inverted pattern. • *PRBS 2^{20}-1 /2^{20}-1 inverted*: This is a pseudo-random bit pattern specified in ITU-T O.150 and O.151 for error performance measurements at the primary bit rate or above. The 2^{20}-1 inverted is a 2^{20}-1 bit wise inverted pattern. • *PRBS 2^{23}-1 /2^{23}-1 inverted*: This is a pseudo-random bit pattern specified in ITU-T O.150 and O.151 for error performance measurements at the primary bit rate or above. The 2^{23}-1 inverted is a 2^{23}-1 bit wise inverted pattern.

Table 4.3: Ethernet Frame Settings

Setting	Description
BERT Patterns	• *PRBS 2^{23}-1 /2^{23}-1 inverted*: This is a pseudo-random bit pattern specified in ITU-T O.150 for special measurement tasks. • *User*: Sets a 32-bit, user configurable word as the transmitted pattern.
User payload	Here it is configured the value of the user payload that is used as the transmitted pattern when *BERT Pattern* is set to *User*.

Some test payloads are byte patterns (*BERT* pattern, *all-Zeroes* pattern) but some others have a more complex structure like the *SLA* test payload. Specifically, the SLA test payload used by test unit is a proprietary extension of the Operations, Administration and Maintenance (OAM) payload defined by standard ITU-T Y.1731.

4.2.Generation of IPv4 Traffic

Without a Network layer, all the Ethernet traffic generated by test unit would be unable lo leave the local network and reach remote networks. The Network Layer, or Layer 3, provides end-to-end connectivity between stations that can use heterogeneous underlying technologies and they are not necessarily attached to the same network. Routers are devices that are designed to manage Layer 3 protocols and data forwarding based on routing tables.

The *Internet Protocol* (IP) is the most popular Layer 3 protocol. It was conceived by the U.S. *Department of Defence* (DoD) during the cold war to facilitate communication between dissimilar computer systems in a reliable way. IP interconnects public or private autonomous systems providing a connectionless service.

There are two IP protocol versions (IPv4 and IPv6). IPv4 addresses can be defined as a subset of the IPv6 addressing space but IPv4 and IPv6 can be regarded as different and incompatible network protocols in any other sense. Currently, Tempo traffic generation functionality is compatible with version four of the IP protocol (IPv4). Traffic analysis include both versions of the IP protocol, IPv4 and IPv6.

The correct operation mode for IPv4 packet generation is the *IP Endpoint* mode. Basically, the traffic generator in *IP Endpoint* mode is configured in the same way than in *Ethernet Endpoint* mode. However, there are some differences to be taken into account:

- In *IP Endpoint* mode, the test equipment becomes a host in an IP network and it has similar properties than any other network equipment. For this reason it is necessary to assign a valid IP profile to the tester either automatically (DHCP) or by hand.

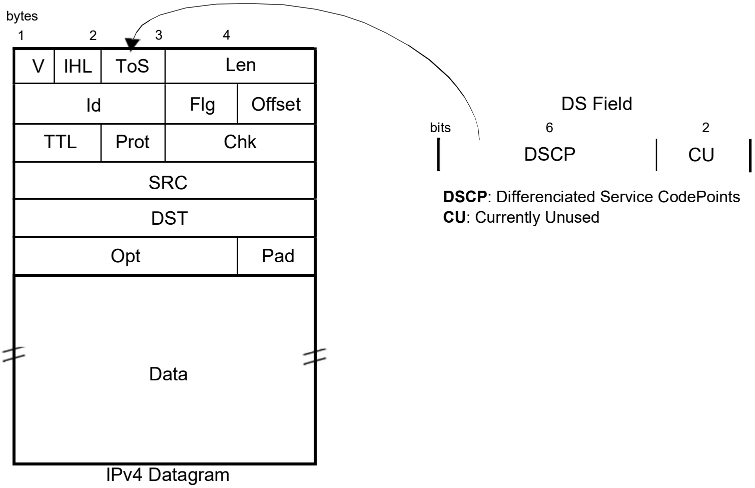


Figure 4.6: IPv4 datagram structure.

- The test equipment is now ready to use some helper protocols to make the configuration process easier. Specifically, the *Address Resolution Protocol* (ARP), configures destination MAC address without user intervention. The *Domain Name Service* (DNS) replaces the configuration of the destination IP addresses by the much simpler domain name configuration.
- Ethernet frames carry IPv4 packets with an specific structure and content. It is necessary to configure the IPv4 packet before it is prepared to generate IP datagrams.
- Optionally IPv4 packets carry one or more MPLS labels. The transmission parameters of MPLS labels have to be configured when they are enabled.

4.2.1. Configuring the Physical and MAC Layers

Physical (layer 1) and MAC (layer 2) configuration is similar in *IP Endpoint* and *Ethernet Endpoint* modes (See section 4.1.1, See section 4.1.2). The only difference is that users now have at their disposal the ARP mechanism to configure the destination MAC address automatically. ARP gets the destination MAC address from the network using the destination IPv4 address by means a broadcast protocol.

To use ARP to set the destination MAC address without user intervention, you have to configure the *Destination MAC address from* to ARP (See section 4.1.2). Once ARP has been configured the test unit generates one or several broadcast ARP requests to compute the destination MAC address. Generation of ARP control traffic is automatic and it is not controlled with the *run* button like it happens with the test traffic.

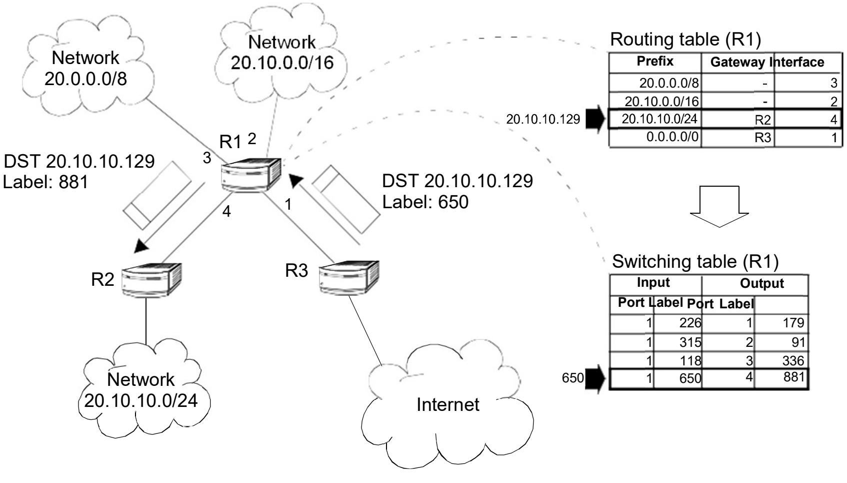
4.2.2. Configuring MPLS

Multi-Protocol Label Switching (MPLS) is a technology designed to speed up IP packet switching in routers by separating the functions of route selection and packet forwarding into two planes:

- *Control Plane*: This plane manages route learning and selection with the help of traditional routing protocols such as *Open Shortest Path First* (OSPF) or *Intermediate System - Intermediate System* (IS-IS).
- *Forwarding Plane*: This plane switches IP packets, taking as a basis short labels prepended to them. To do this, the forwarding plane needs to maintain a switching table that associates each incoming labelled packet with an output port and a new label.

The traditional IP routers switch packets according to their routing table. This mechanism involves complex operations that slow down switching. Specifically, traditional routers must find the longest network address prefix in the routing table that matches the destination of every IP datagram entering the router.

On the other hand, MPLS routers, also known as *Label-Switched Routers (LSR)*, use simple, fixed-length label forwarding instead of a variable-length IP network prefix for fast forwarding of packetized data.



Routing table (R1)

Prefix	Gateway	Interface
20.0.0.0/8	-	3
20.10.0.0/16	-	2
20.10.10.0/24	R2	4
0.0.0.0/0	R3	1

Switching table (R1)

Input		Output	
Port	Label	Port	Label
1	226	1	179
1	315	2	91
1	118	3	336
1	650	4	881

Figure 4.7: Traditional routers have to perform complex operations to resolve the output interface of incoming packets. LSRs resolve the output interface with the help of a simple switching table.

MPLS enables the establishment of a special type of virtual circuits called *Label-Switched Paths* (LSP) in IP networks. Thanks to this feature, it is possible to implement resource management mechanisms for providing hard QoS on a per-LSP basis, or to deploy advanced traffic engineering tools that provide the operator with tight control over the path that follows every packet within the network. Both QoS provision and advanced traffic engineering are difficult, if not impossible to solve in traditional IP networks.

To sum up, the separation of two planes allows MPLS to combine the best of two worlds: the flexibility of the IP network to manage big and dynamic topologies automatically, and the efficiency of connection-oriented networks by using pre-established paths to route the traffic in order to reduce packet process on each node.

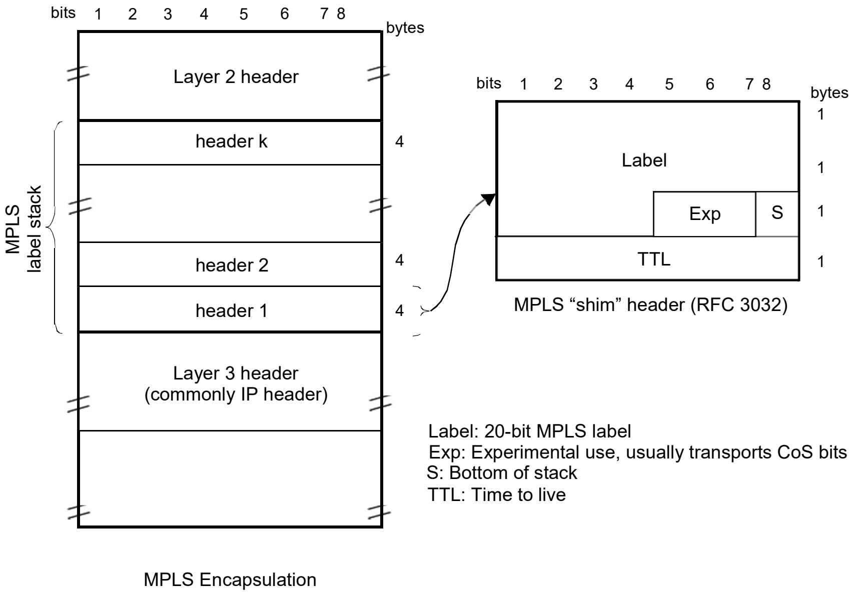


Figure 4.8: MPLS “shim” header format. The label is usually inserted between layer-2 and layer-3 headers.

The test unit can be configured to generate and analyse MPLS packets carrying one or two labels. The configuration procedure is as follows:

1. Make sure that your tester is connected to the network. The physical layer must be up and working (See section 4.1.1).
2. From the *Home* panel, go to *CONFIG*,
   The test port settings panel is displayed.
3. Select either Port A or Port B to enter in the port specific configuration.
4. Enter in the *MPLS* menu.
   All settings related with MPLS packet generation configuration are displayed.

5. Select one of the traffic flows between *Flow #1* and *Flow #8* to enter in the flow specific configuration.

Table 4.4: MPLS Settings

Setting	Description
Stack configuration	Configures the size of the MPLS label stack for the current flow. Both single and double stack configurations are supported. • *Off*: Disables MPLS generation in the current flow. • *Single MPLS label*: Enables single MPLS label generation in the current flow. The user is expected to configure the bottom label, traffic class and TTL for the MPLS header. • *Double MPLS label*: Enables double MPLS label generation in the current flow. The user is expected to configure both the top and bottom label, traffic class and TTL for the MPLS headers.
Bottom label	MPLS label used for switching traffic in the bottom MPLS header. This field is enabled when the user has selected *Single MPLS label* or *Double MPLS label* in *Stack configuration*.
Bottom traffic class	Contains the traffic class identifier for the bottom MPLS header. It was first thought that this field could carry the 3 Type-of-Service (ToS) bits defined for Class of Service (CoS) definition in the IP version 4, but currently, the ToS field is being replaced by 6-bit *Differentiated Services Code Points* (DSCP). This means that only a partial mapping of all the possible DSCPs into this field is possible. This field is enabled when the user has selected *Single MPLS label* or *Double MPLS label* in *Stack configuration*.
Bottom TTL	This field contains a *Time To Live* value for the bottom MPLS header. The value of this field is decremented by one unit every time the packet traverses an LSR. The packet is discarded if the value reaches 0. This field is enabled when the user has selected *Single MPLS label* or *Double MPLS label* in *Stack configuration*.
Top label	This field contains the MPLS label used for switching traffic in the top MPLS header. This field is enabled only if the user has selected *Double MPLS label* in *Stack configuration*.

Table 4.4: MPLS Settings

Setting	Description
Top traffic class	This field contains the traffic class identifier for the top MPLS header. It was first thought that this field could carry the 3 Type-of-Service (ToS) bits defined for Class of Service (CoS) definition in the IP version 4, but currently, the ToS field is being replaced by 6-bit *Differentiated Services Code Points* (DSCP). This means that only a partial mapping of all the possible DSCPs into this field is possible. This field is enabled only if the user has selected *Double MPLS label* in *Stack configuration*.
Top TTL	This field contains a *Time To Live* value for the top MPLS header. The value of this field is decremented by one unit every time the packet traverses an LSR. The packet is discarded if the value reaches 0. This field is enabled only if the user has selected *Double MPLS label* in *Stack configuration*.

6. Configure *Stack configuration* to *Off* to disable MPLS generation over the current flow. Set *Single MPLS label* or *Double MPLS label* to generate IP packets carrying one or two MPLS labels.
7. If you have configured *Single MPLS label* in the previous step, type the correct values for *Bottom label, Bottom traffic* class and *Bottom TTL*. If you have configured *Double MPLS label,* enter the values for *Bottom label*, *Bottom traffic class*, *Bottom TTL*, *Top label*, *Top traffic class* and *Top TTL*.

4.2.3. Configuring the Port Local Network Profile

The test equipment requires a local IP profile when it is operating in *IP Endpoint* mode. Even if the traffic generator has been configured to work with a custom IP address (different to the local IP address), the equipment still requires an internal address for some tests like the *IP Ping* or the *Traceroute*. Furthermore, some control and signalling protocols may work with the information stored in the local IP profile only. Specifically, it must be noticed that the test unit only responds to ARP and ICMP echo requests from the IP address and VID configured in the local profile. This fact must be taken into account when the source IP address is configured to something different to *Local* (*Network layer* settings) and *Encapsulation* is set to something different to *Local profile* (*Frame layer* settings).

Configuration of the local IP profile is available form the port specific settings within the Setup menu (See section 2.3).

4.2.4. Configuring the IPv4 Datagram

The IPv4 packet content is set much in the same way that the MAC frame content. However, in this case, MAC addresses are replaced by IPv4 addresses. Of course, IPv4 datagrams have their own structure and they contain some fields not present in Ethernet frames.

Table 4.5: IPv4 Packet Settings

Setting	Description
Source IPv4 address from	Establishes the origin of the source IPv4 address for the current stream. There are two possible settings: • *Local*: The source address is set to the IPv4 address configured in the port local profile. The local address may be either configured by means the DHCP protocol or in may be static. • *Manual*: The source address is set to the value configured in *Source IPv4 address*. Use manual IPv4 addresses if you want to simulate traffic generated by an equipment different to the tester or, in multi-stream operation, to simulate traffic transmitted from different hosts. Probably, you will want to avoid duplicated IP addresses in your network. For this reason, make sure that no other equipment is using the manually configured IPv4 address. • *Remote*: This option is available only in RFC 2544 or eSAM downstream asymmetric tests (See section 7.4). It configures the source IPv4 address to be the far end address. It must be taken into account that in downstream asymmetric tests, the far end is configured for traffic generation. This setting corresponds with traffic to be generated not in the local unit but in a different one. • *Port A / Port B*: Configures the opposite port in the same unit as the destination for the traffic. Port B is displayed as one of the accepted destinations for Port A and Port A is shown in Port B with the same purpose.
Source IPv4 address	Source IPv4 address carried by the packets generated in the current stream if *Source IPv4 address from* is set to *Manual*. The address is entered in decimal, four-dotted format. Any address between 0.0.0.0 and 255.255.255.255 is admitted as a source IPv4 address.

Table 4.5: IPv4 Packet Settings

Setting	Description
Destination IPv4 address from	Establishes the origin of the destination IPv4 address for the current stream. There are three different settings available for configuration: • *Manual*: The destination address is set to the value configured in *Destination IPv4 address*. • *Range*: Test data in the current stream is transmitted to a group of IPv4 addresses configured with *Destination IPv4 address* and *Address range size*. Use this option if you want to deliver the test data sequentially to many different destinations. • *Host name*: Uses the Domain Name Service (DNS) to set the destination IP address by using descriptive alphanumeric strings. The DNS mechanism requires intervention of at least one DNS server. The DNS server IP address has to be configured in the local port profile either statically or by means DHCP. • *Remote*: This option is available only in RFC 2544 or eSAM upstream asymmetric tests (See section 7.4). It configures the destination IP address to be the far end address.
Destination IPv4 address	Destination IPv4 address carried by the packets generated in the current stream if *Destination IPv4 address from* is set to *Manual*. The address is entered in decimal, four-dotted format. Any address between 0.0.0.0 and 255.255.255.255 is admitted as a destination IPv4 address.
Destination IPv4 address (DNS)	Destination IPv4 address carried by the packets generated in the current stream if *Destination IPv4 address from* is set to *Host name*. This is a read only field that it cannot be edited directly. It displays the result of the DNS name resolution carried out with the host name configured in *Destination host name.*

Table 4.5: IPv4 Packet Settings

Setting	Description
Address range size	Configures the number of IPv4 addresses within an address range. This control is valid only if *Destination type* is set to *Range*. In this case, the IP datagrams transmitted in the current stream will contain as many destination addresses as previously configured in this field. The destination IP address is increased by one unit for each transmitted frame starting with the value configured in *Destination IPv4 address*. If there are no more addresses left in the range, transmission returns to the initial address and starts the process from the beginning. Transmission of destination IPv4 address ranges is compatible with transmission of destination MAC address ranges but the address number of the MAC address range is always fixed to the same number that the IP range. It is not possible to transmit a destination MAC address range with a single IPv4 address.
Destination host name	Domain name to be used as a destination if *Destination IPv4 address from* is set to *Hostname*. Unlike IP addresses, domain names are easy-to-remember alphanumeric strings but they have to be translated to IP addresses before any packet can be sent to the destination. The translation process requires the intervention of at least one DNS server. The DNS server IP address has to be configured in the local port profile either statically or by means DHCP.
DSCP	Differentiated Services Code Point. It is 6-bit class of service (CoS) field defined to set packet groups with different priorities or to provide specific treatments to special packets within a network or an administrative domain. Any value from 0 to 63 is allowed for this field. Specific actions to be carried out on frames with different DSCPs depend on the network and the service provider.
TTL	Initial Time To Live value configured in the packets transmitted in the current stream. The TTL is decreased by one unit each time it lefts a network node. If the value reaches zero, then the packet is discarded. The TTL is then a measure of the number of nodes the packet is allowed to transverse before reaching its destination.

Table 4.5: IPv4 Packet Settings

Setting	Description
UDP	Enables or disables transmission of the User Datagram Protocol (UDP) in the current stream. The UDP is defined in RFC 768 and it is a lightweight transport protocol for unreliable data transmission. RFC 768 defines an eight-byte fixed length header for UDP that is generated when UDP generation is enabled in the stream. If UDP generation is on, the *Transport protocol* field is set to 17. This value cannot be edited by the user.
Transport protocol	This setting contains an 8-bit word that constitutes the protocol identifier to be transmitted by the traffic generator. TCP uses 6 as the protocol number, UDP uses 17 for the same purpose and ICMP uses number 1. However, the payload structure does not match the structure corresponding to these protocols even if the correct protocol number is configured. To enable UDP header and payload generation, enable UDP in the current stream.
Source port	Source transport layer port transmitted in the UDP header in the current stream. Ports are service identifiers used to multiplex data from different applications generated by IP hosts. The tester supports source port generation for UDP streams only.
Destination port	Destination transport layer port transmitted in the UDP header in the current stream. Ports are service identifiers used to multiplex data from different applications generated by IP hosts. The tester supports destination port generation for UDP streams only.

All the IPv4 datagram configuration lays within the *Network* menu. The network menu is not enabled unless the port is configured in TX / RX mode. The procedure to follow to configure the IP datagram is described below:

1. Make sure that your tester is connected to the network. The physical layer must be up and working (See section 4.1.1). Check that your tester is operating in *IP Endpoint* mode (See section 2.1) and that the port is in *TX / RX*.
2. From the *Home* panel, go to *CONFIG*,
   The test port settings panel is displayed.
3. Select *Port A* or *Port B* to enter in the port specific configuration.
4. Enter in the *Network layer* menu.

5. Select one of the traffic flows between *Flow A1* and *Flow A8* (or *Flow B1* and *Flow B8* in *Port B*) to enter in the flow specific configuration.
   All settings related with network configuration in the current flow are displayed.
6. Enter the source IP address with the help of the *Source IPv4 address from* and *Source IPv4 address* controls. You can configure the IP address from the local IP profile as the source address or enter a custom address.
7. Enter the destination IPv4 address or addresses by using the *Destination IPv4 address from*, *Destination IPv4 address*, *Address range size* and *Destination host name*. If you choose to generate a destination address range you will be requested to enter the number of addresses that made up the range. If you choose to enter the destination as a host name rather than an IPv4 address, you will be requested to enter a valid domain name.
8. Configure the DSCP and TTL if necessary.
9. Enable or disable UDP generation and analysis with the help of the *UDP*control.
10. If you have enabled UDP, enter the *Source Port* and *Destination Port* to be used in the generated UDP packets.
11. If you have not enabled UDP, configure the *Transport Protocol* code.
12. If necessary, repeat the IPv4 configuration process for one or more traffic flows (*Flow A1* to *Flow A8* or *Flow B1* to *Flow B8*, depending on the test port) available from the *Network layer* menu.

4.2.5. Setting the Bandwidth Profile

Setting the bandwidth profile in *IP Endpoint* mode is the same that in *Ethernet Endpoint* mode (See section 4.1.3)

4.2.6. Choosing the Test Payload for IPv4

The test unit includes special packet payloads and patterns required for all usual applications, including BER tests and SLA tests. Payloads and patterns available in *IP Endpoint* mode are similar than in *Ethernet Endpoint* mode (See section 4.1.4). However, there is a difference concerning the SLA payload. While in *Ethernet Endpoint* the SLA payload is defined as an extension of the ITU-T Y.1731 structure, in *IP Endpoint*, this payload is Calnex proprietary. In practical terms, the structure of the SLA payload should not make any difference when testing.

4.3. Event Insertion

Sometimes it is necessary to insert events in the generated signal to stress the DUT/ SUT. The test unit implements extended event insertion capabilities. The procedure to set event insertion with the test unit is as follows:

1. From the *Home* panel, go to *TEST*,
   The *Test* configuration panel is displayed.

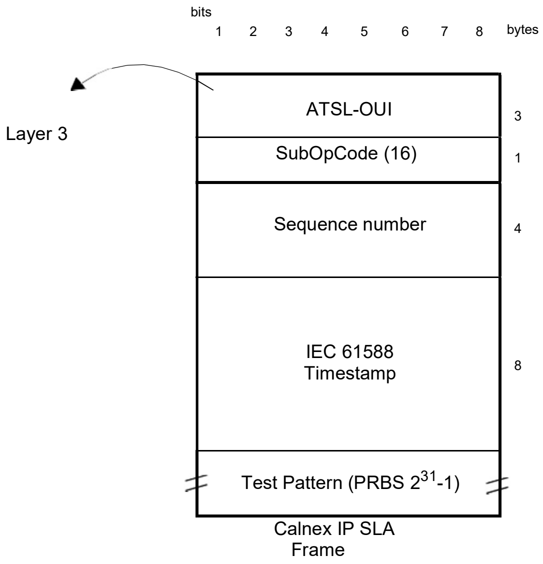


Figure 4.9: Calnex payload for SLA tests (IP Endpoint mode).

2. Select *Insertion*
   The event insertion menu is displayed.
3. Select the event to be inserted with the help of the *Event to be inserted* menu item.
4. Select the insertion mode for the event selected in the previous step with the help of the *Mode* menu item. Available insertion modes are: *Single*, *Rate*, *Burst* or *Random*.
5. Configure the insertion parameters with the help of the *Event rate*, *Number of frames*, *Probability (%)* and *Frame size (bytes)* menu items.
6. Start insertion by pressing the *event* button.
   Note: Depending on the insertion mode, event insertion will finish automatically or you will need to press *event* a second time to stop.

Table 4.6: Event Insertion Settings

Setting	Description
Insert to	Sets the test port where the event is going to be inserted.

Table 4.6: Event Insertion Settings

Setting	Description
Event to be inserted	Contains a selection list with events the user can choose for insertion in the transmitted data stream.The events available are: • *None*: Disables event insertion in the target port and flow. No event will be generated in case the user presses *event*. • *FCS*: Generates *Frame Check Sequence* errors. A frame with a FCS error is a frame with a legal size which contains an invalid FCS field. Under normal circumstances, FCS errors are caused by transmission errors. An optical Ethernet link with a poor power budget may experience FCS errors • *IPv4 checksum*: Generates frames with an invalid IPv4 header checksum. In normal circumstances, in Ethernet networks, IP checksum errors are related with corrupted traffic generation. IPv4 checksum error insertion is available only in *IP endpoint* mode. • *Undersized frames*: This event is used to generate frames shorter than the minimum legal size (64 bytes). The frame size of an undersized frame is configured through the *Frame size (bytes)* field. • *UDP checksum*: Generates frames with an invalid UDP checksum. Under normal circumstances, UDP checksum errors are related with corrupted traffic generation. UDP checksum error insertion is available only in *IP endpoint* mode. • *TSE*: Generates *Test Sequence Errors*, One TSE is equivalent to a single bit difference between the transmitted and the received test pattern (PRBS or other). TSE event insertion is not available if the target port transmitter is not configured for transmission of a BER test pattern. • *Pause frames*: Generates Ethernet pause frames to trigger the activation of the flow control mechanism in the peer equipment.

Table 4.6: Event Insertion Settings

Setting	Description
Mode	Configures the way events are inserted in the outgoing signal. Depending on whether the insertion event is an anomaly or a defect there are different insertion modes. For anomalies, the insertion modes are: • *Single*: A single event is inserted. Event insertion is triggered when the *event* key is pressed. • *Burst*: A burst events a configurable number of events is inserted. Burst start is triggered with the *event* key. • *Rate*: Events are inserted with a configurable rate. Insertion is deterministic (the time interval between consecutive events is a constant). Insertion starts if the *event* key is pressed. Insertions stops when the *event* key is pressed again. • *Random*:The number of events generated is random.For each insertion opportunity, the transmitter decides if the event is inserted or not depending on a user configurable insertion probability.
Event rate	If the insertion mode has been set to *Rate*, this fields sets the rate at which events are inserted in the outgoing signal. The rate is entered in scientific notation: A x 10^{-B} In this notation B is a number between -3 and -9 (both included) and A is a real positive number smaller than 10.
Number of frames	If insertion mode has been set to *Burst*, this field sets the number of events that makes up the burst. For example a burst of 10 bit errors is made of ten consecutive TSE errors.
Probability (%)	If the insertion mode is set to *Random,* this is the probability of a single event occurrence expressed as a percentage.
Frame size (bytes)	If *Event to be inserted* has been configured to *Undersized frames*, this field configures the frame length corresponding to these undersized frames expressed in bytes. It is a number between 32 and 63.
Pause Time (quanta)	Configures the pause time in an Ethernet pause frame in “quanta” units. One quanta is equivalent to 512 bit times.

Chapter 5
Basic Frame Analysis

Calnex Tempo can be used to get advanced traffic counts and statistics about Ethernet and IP networks operating at rates up to 10 Gb/s. These statistics include frame and error counts, bandwidth statistics, quality of service statistics, frame size statistics and other results.

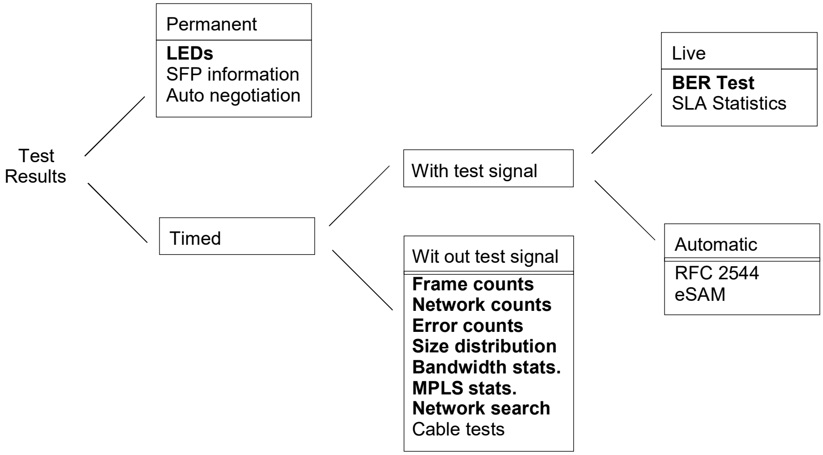


Figure 5.1: Statistics and counts available in Tempo.

Test results supplied by the test unit can be classified in many different ways. One of them is to think in test results that require a previous test start action with the *run* button (*timed* results) or results which are always available when the equipment is on (*permanent* results). A second approach is to classify test results in those which depend on an special test signal transmitted from an special traffic generator and results available in any case, even if there is no test signal available foranalysis.

This chapter deals mainly with timed results which does not require test signals and the closely related LED results even if these are permanent results. At the end of the chapter BER test results are also addressed, but these are different in nature to all other measurements because they require a BERT payload / pattern received in the test interface. These test may be generated by the same test unit or a remote tester.

5.1. Global Counts and Statistics

Global frame counts and statistics are those not associated to any particular stream. Some global statistics have a per-stream statistic counterpart. Examples of this are the bandwidth statistics and some frame counts.

Global counts and statistics for Port A and Port B are identical. Global frame statistics are controlled by the *run* button. That means that results are not collected if a test is not started before. Once the test is running results are upgraded in real time.

Counts and statistics described in this section are available both in endpoint (*Ethernet Endpoint*, *IP Endpoint*) and through mode.

5.1.1. Frame Counts

Frame counts provide information about how many frames have been received in the test interface from the beginning of the test. These counts are also useful to classify the frames received in different families.

To display the transmitter statistics follow these steps:

1. From the *Home* panel, go to *RESULTS*,
   The test port results panel is displayed.
2. Select either *Port A or Port B* to enter in the port specific results.
3. Enter in *Frame layer statistics*.
4. Check the *TX frames*, *RX frames*, *Unicast frames*, *Multicast frames*, *Broadcast frames*, *VLAN*, *IEEE 802.1ad*, *Q-in-Q*, *Control frames*, *Pause frames* and *BPDU* counters.

Table 5.1: Global Frame Statistics

Metric	Description
TX frames	Total number of frames transmitted by one tester port since the test started.
RX frames	Total number of frames received by one tester port since the test started.
Unicast frames	Total number of Ethernet unicast frames received from the beginning of the test. Unicast frames are recognised because they contain a unicast destination MAC address. Unicast MAC frames have their multicast bit set to ‘0’. The multicast bit of a MAC address is the least significant bit of the more significant address byte.

Table 5.1: Global Frame Statistics

Metric	Description
Multicast frames	Received Ethernet multicast frames from the beginning of the test. Ethernet multicast frames have their multicast bit in their destination MAC address set to '1'. The multicast bit of a MAC address is the least significant bit of the more significant address byte.
Broadcast frames	Total number of Ethernet broadcast frames received from the beginning of the test. Broadcast frames carry the broadcast Ethernet address (*ff:ff:ff:ff:ff:ff*) in the destination field.
VLAN	Total number of Ethernet VLAN frames transmitted from the beginning of the test. IEEE 802.1Q VLAN frames contain an special Ethertype (Type / Length field) value (*0x8100*).
IEEE 802.1ad	Total number of *Provider Bridge* (PB) frames received from the beginning of the test. PB frames are defined by standard IEEE 802.1ad. PB frames contain two VLAN tags referred as C-VLAN and S-VLAN. The C-VLAN carries Type *0x8100*. The S-VLAN has the special Type *0x88a8*.
Q-in-Q	Total number of double-tagged VLAN frames received from the beginning of the test. Q-in-Q frames contain an S-VLAN and a C-VLAN but they are not compliant with the IEEE 802.1ad standard. This standard requires the Type field for the S-VLAN to be *0x88a8* but not-standard Q-in-Q frames use different values like *0x8100*, *0x9100*, *0x9200* or *0x9300*.
Control frames	Total number of Ethernet MAC control and supervision frames received from the beginning of the test. Ethernet control frames are recognised due to an special Ethertype (Type / Length field) value (*0x8808*).
Pause frames	Total number of Ethernet *Pause* frames received from the beginning of the test. Pause frames are an special type of control frames and therefore their Ethertype is 0x8808. The specific features of *Pause* frames is that their *Opcode* field is 0x0001 and their destination MAC address is *01:80:c2:00:00:01* (a multicast MAC address).

5.1.2. Error Counts

Tempo is prepared to get any defect or fault in the received data stream. These faults include invalid checksum, alignment or size and frame structure defects. If configured in pass-through mode, the test unit, automatically drops frames with errors but these are still counted and presented in the error statistics panels. To access to the error statistics:

1. From the *Home* panel, go to *RESULTS*,
   The test port results panel is displayed.
2. Select either *Port A or Port B* to enter in the port specific results.
3. Enter in *Error statistics*.
4. Check the *FCS*, *Undersized*, *Oversized*, *Jabbers*, *IPv4 / IPv6 errors*, *UDP errors* and *TCP errors* counters.

Table 5.2: Global Error Counts

Metric	Description
FCS	Count of all the FCS errors detected from the beginning of the test. A frame with a FCS error is a frame with a legal size which contains an invalid FCS field. FCS errors are caused by transmission errors. An optical Ethernet link with a poor power budget may experience FCS errors
Undersized	Total number of received frames which are smaller than 64 bytes.
Oversized	Total number of received frames which are larger than the configured MTU.
Jabbers	Jabber count from the beginning of the test. A Jabber is defined as a frame greater than 1518 bytes with a bad CRC.
IPv4 / IPv6 errors	Displays information about the total number of errored IPv4 and IPv6 packets. An IPv4 or IPv6 packet is declared an errored packet if it is improperly built: Datagram header has an unexpected structure, field values are different to the expected ones or it has an unexpected length. An IPv4 datagram is also considered to be invalid if it contains checksum errors.

Table 5.2: Global Error Counts

Metric	Description
UDP errors	Displays information about the total number of errored UDP packets. UDP packets are considered to contain errors if either their structure or their content is invalid. For UDP, this means that the packet has an unexpected length or it contains checksum errors.
TCP errors	Displays information about the total number of errored TCP packets. TCP packets are considered to contain errors if either their structure or their content is invalid. For TCP, this means that the packet contains checksum errors.

5.1.3. Network Counts

The *Network layer statistics* panel has similar purpose than the *Frame layer statistics* but in this case it displays counters related with the IP layer rather than with Ethernet. Network statistics are not available in *Ethernet Endpoint* mode because the IP structure is neither generated nor decoded in this operation mode.

Table 5.3: Global Network Statistics

Metric	Description
IPv4 / IPv6 TX	Aggregated number of transmitted IPv4 and IPv6 packets since the last test start. IPv4 packets are encapsulated in Ethernet frames carrying the 0x0800 Type. IPv6 packets are encapsulated with the Ethertype field set to 0x86dd.
IPv4 RX	Total number of received IPv4 packets since the last test start. IPv4 packets are encapsulated in Ethernet frames carrying the 0x0800 Type.
IPv4 frags	Counter that increases every time a fragment corresponding to an IPv4 fragmented packet is received. A fragment is detected because the *More Fragments* (MF) flag is enabled in the frame.

Table 5.3: Global Network Statistics

Metric	Description
IPv6 RX	Total number of received IPv6 packets since the beginning of the test with RUN. IPv6 packets are encapsulated in Ethernet frames carrying the 0x86dd Type.
Unicast pkts.	Aggregated count of unicast IPv4 and IPv6 packets received from the beginning of the test. An IPv4 unicast packet is a packet directed to a unicast IPv4 address. An IPv4 unicast address is any valid, not-broadcast Class A (1.0.0.1 - 126.255.255.254), Class B (128.1.0.1 - 191.255.255.254) or Class C (192.0.0.1 - 192.255.254.254) address. An IPv6 unicast packet is a packet directed to a unicast IPv6 address. All non-multicast IPv6 (prefix ff00::/8) packets are considered to be unicast.
Multicast pkts.	Aggregated count of unicast IPv4 and IPv6 packets received from the beginning of the test. An IPv4 multicast packet is a packet directed to a multicast IPv4 address. An IPv4 multicast address is any valid Class D (224.0.0.0 - 239.255.255.255) address. An IPv6 multicast packet is a packet directed to a multicast IPv6 address. IPv6 multicast addresses is an address starting with the ff00::/8 prefix.
Broadcast pkts.	Total count of broadcast IP packets received from the beginning of the test. An IPv4 broadcast packet is a packet directed to the currently configured network broadcast address or the global broadcast address (255.255.255.255). The network broadcast address is the IPv4 address that has all the host bits set to 1. There is no definition for IPv6 multicast addresses. For this reason IPv6 statistics are not included in this result field.
UDP	UDP packets or segments are IP packets carrying the User Datagram Protocol (UDP) defined in RFC 768. The protocol number assigned to UDP is 17.

Table 5.3: Global Network Statistics

Metric	Description
ICMP / ICMPv6	Aggregated count of ICMP and ICMPv6 messages received from the beginning of the test. ICMP packets carry Internet Control Message Protocol (ICMP) messages defined in RFC 792. ICMPv6 messages carry the version 6 of Internet Control Message Protocol defined in RFC 4443. The protocol number assigned to ICMP is 1. For ICMPv6 the protocol number is 58.
TCP	TCP packets or segments are IP packets carrying the User Datagram Protocol (TCP) defined in RFC 793. The protocol number assigned to TCP is 6.

To display the network statistics corresponding to the last (or current) test, follow these steps:

1. From the *Home* panel, go to *RESULTS*,
   The test port results panel is displayed.
2. Select either *Port A or Port B* to enter in the port specific results.
3. Enter in *Network layer statistics*.
4. Check the *IPv4 TX*, *IPv4 RX*, *IPv4 frags*., *IPv6 RX*, *Unicast pkts.*, *Multicast pkts.*, *Broadcast pkts.*, *UDP ICMP / ICMPv6* counters.

5.1.4. Bandwidth Statistics

Bandwidth statistics inform about how many frames and bits you are receiving per time unit and how much of the available bandwidth is being used by the traffic. Traffic statistics are supplied at many different transmission layers, including Ethernet, IP and UDP. IP and UDP is closer to the amount of usable data and Ethernet statistics are more related with the bandwidth available for transmission.

Bandwidth statistics are timed measurements, you need to run a test to start collecting results. In order to access to these results follow these steps:

1. From the *Home* panel, go to *RESULTS*,
   The test port results panel is displayed.
2. Select either *Port A or Port B* to enter in the port specific results.
3. Enter in *Bandwidth statistics*.
4. Select *General statistics*.

5. Check the *Eth. (current)*, *Eth. (min.)*, *Eth (max.)*, *Eth. unicast*, *Eth. multicast*, *Eth. broadcast*, *IPv4 (current)*, *UDP (current)* results.

Table 5.4: Bandwidth Statistics

Metric	Description
Eth. (current)	Total amount of Ethernet traffic received during the last second computed in bits per second, frames per second andas a percentage of the total channel capacity. The frame bits considered in Ethernet traffic statistics are between the first bit of the destination address field to the last bit of the FCS field. The current Ethernet traffic counter requires previous initialization of a test with the *run* button.
Eth. (max)	Peak value of Ethernet traffic registered from the beginning of the test. The *Ethernet (max)* value displays the maximum value found in the *Ethernet (current)* field since the test started. The *Ethernet (max)* is displayed in three different units: bits per second, frames per second and percentage of the overall channel capacity.
Eth. (min)	Minimum value of Ethernet traffic registered from the beginning of the test. The *Ethernet (min)* value displays the minimum value found in the *Ethernet (current)* field since the test started. The *Ethernet (max)* is displayed in three different units: bits per second, frames per second and percentage of the overall channel capacity.
Eth. unicast	Total amount of unicast Ethernet traffic received during the last second computed in frames per second. Unicast frames are recognised because they contain a unicast destination MAC address. Unicast MAC frames have their multicast bit set to ‘0’. The multicast bit of a MAC address is the least significant bit of the more significant address byte.
Eth. multicast	Total amount of multicast Ethernet traffic received during the last second computed in frames per second. Ethernet multicast frames have their multicast bit in their destination MAC address set to ‘1’. The multicast bit of a MAC address is the least significant bit of the more significant address byte.

Table 5.4: Bandwidth Statistics

Metric	Description
Eth. broadcast	Total amount of broadcast Ethernet traffic received during the last second computed in frames per second. Broadcast Ethernet frames carry the broadcast Ethernet address (*ff:ff:ff:ff:ff:ff*) in the destination field.
IPv4 (current)	Total amount of IPv4 traffic received during the last second computed in bits per second, frames per second and as a percentage of the overall channel capacity. The current IPv4 traffic counter requires previous initialization of a test with the RUN button.
IPv6 (current)	Total amount of IPv6 traffic received during the last second computed in bits per second, frames per second and as a percentage of the overall channel capacity. The current IPv6 traffic counter requires previous initialization of a test with the RUN button.
UDP (current)	Total amount of traffic associated to the Ethernet / IP / UDP payloads computed in bits per second, frames per second and as a percentage of the overall channel capacity. The current *User traffic* counter requires previous initialization of a test with the RUN button.

5.1.5. Frame Size Distribution

Frame size is important because it tells how a network is used. Some applications, like VoIP use short frames while most data applications based on a client / server architecture use short frame lengths for the client requests and long frames for the server replies. The Calnex Tempo provides frame size results as described in standard RFC 2819. The procedure for displaying the received frame size distribution is as follows:

1. From the *Home* panel, go to *RESULTS*,
   The test port results panel is displayed.
2. Select either *Port A or Port B* to enter in the port specific results.
3. Enter in *Frame size histogram*.
4. Check the frame size intervals: *64 or less*, *65 - 127*, *128-255*, *256 - 511*, *512-1023*, *1024 - 1518, 1519 - 1522*, *1523-1526*, *1527 - MTU*.

5.1.6. MPLS Statistics

Network statistics and all other results are not affected when the received traffic contains MPLS labels. For example, IPv4 datagrams are still IPv4 packets when they have one or more MPLS labels and they are still recognised as unicast, multicast or broadcast packets when this happens. MPLS test results are limited to an indication of the presence of MPLS in the received traffic and some statistics about the MPLS stack size. To display the MPLS statistics follow these steps:

1. From the *Home* panel, go to *RESULTS*,
   The test port results panel is displayed.
2. Select either *Port A or Port B* to enter in the port specific results.
3. Enter in *MPLS statistics*.
4. Check the *MPLS labels per packet (min.)* and *MPLS labels per packet (max.)* counters.

Table 5.5: MPLS statistics

Metric	Description
MPLS labels per packet (min.)	Minimum number of MPLS labels per packet found in the received traffic from the beginning of the test. If it has been received at least one frame without MPLS labels, this result will be set to 0.
MPLS labels per packet (max.)	Maximum number of MPLS labels per packet found in the received traffic from the beginning of the test.

5.2. Using the Network Search Capability

Network Search is an optional monitoring tool for the test unit that reports the top MAC, IPv4 and IPv6 addresses found in the network. Also, if you are connected to a tagged interface, the network search can be configured to collect the most viewed VLANs. Network search can be used to look for an specific traffic flow in your network or maybe as a preliminary analysis tool before filtering the interesting traffic flows and getting detailed statistics about them. In fact, the Network Search capability is prepared to be used as a preliminary analysis tool: Once the traffic search has finished the user can choose which filters to configure following the results of the network search. All this is done by a simple key press. Network Search is used in the following way:

1. From the *Home* panel, go to *CONFIG*,
   The test port settings panel is displayed.
2. Select either *Port A* or *Port B* to enter in the port specific configuration.
3. Go to *Search network by* and define your search field: *Source MAC address*, *Destination MAC address*, *VLAN, Source IPv4 address*, *Destination IPv4 address, Source IPv6 address, Destination IPv6 address*.
   Note: *Source IPv4 / IPv6 addresse*s and *Destination IPv4 / IPv6 addresses* are available only if you are working in an IP mode (*IP endpoint* or *IP through*). You can configure *VLAN* even if you are not connected to a tagged interface but you will not collect any VLAN information when you start the measurement. In order to disable the network search in the current port set *Search network* by to *Off*.

Note: You can run one *Network search* in *Port A* and one in *Port B*. To do that, simply configure a search field for each port.

4. Leave the previous panel to *Home* and go to *RESULTS*.
   The test port results panel is displayed.
5. Select either *Port A or Port B* to enter in the port specific results.
6. Go to *Network Search*.
7. Start a test by pressing *Run*.
   The network search panel is filled with popular addresses or VLANs found in your network. There is a percentage that indicates how many times each address or VLAN has been found to the time.
8. Finish the search by pressing *Run* a second time.
9. Choose which addresses or VLANs will be used to configure the filters on the receiver.
10. Press the *Configure* contextual button to configure the filters with the previously collected data. To get extended information about these filters you will need to run a second measurement once they have been configured with this action (See chapter 6).

5.3. The LEDs Panel

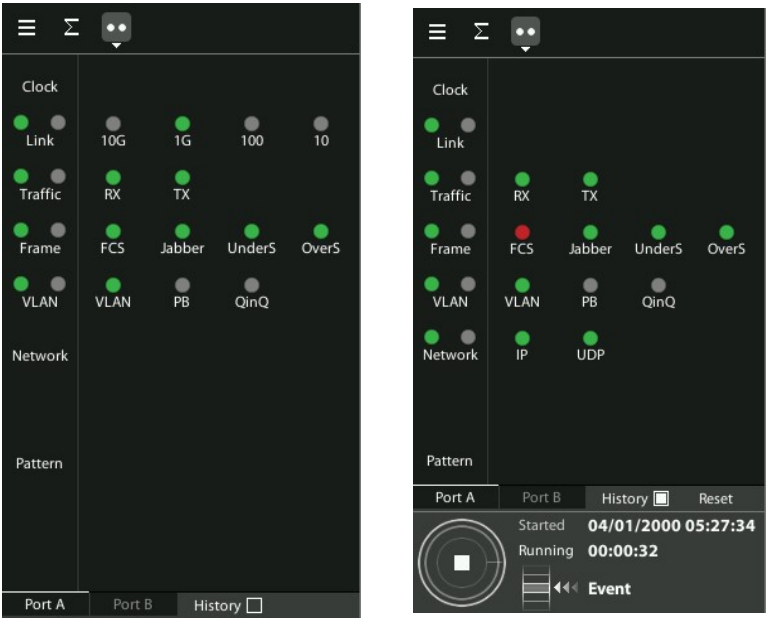
The LEDs panel offers a quick view of the current Tempo connection and operation status. They are permanent indicators. That means that no test has to be started to get the information from the LEDs.

There are two hardware global summary LEDs in the equipment (one for Port A and one for Port B), six summary LEDs for each test port (*Link*, *Traffic*, *Frame*, *VLAN, Network* and *Pattern*). These summary LEDs summarize the information of the events shown in the LEDs panel. To display the LEDs panel use the LEDS key or the corresponding active area in the screen. If the LEDs panel is already visible press again to return to the previous screen.

The LEDs have two operation modes:

- *Live*: Events are shown in real time. If something happens the corresponding LEDs change their colour to signal the event. LEDs return to their original status once the event disappears.
- *History*: The LEDs keep their original Anomaly / Defect status when the event disappears. This is useful when the tester is left a long time under operation and the user wants to receive quick feedback of past events.

The live or history modes can be configured from the LEDs panel by means the contextual keyboard. The *History* check box sets or unsets the history mode. If the history mode is enabled, then the Reset button resets the LEDs history.



(a) (b)

Figure 5.2: Calnex Tempo LEDs panel.

Orange is used to signal anomalies and red indicates defects but there are more possible LED status:

- 🟩: OK, the event or events that correspond with the LED are not found in the incoming signal.
- 🟧 and 🟥: This is the colour displayed if faulty conditions are found in the sig- nal. Conditions marked with 🟥 tend to be more important than the ones marked with 🟧.
- ▬: Shows that no operation condition can be established due to the lack of matching traffic for the corresponding event. For example, the FCS led is ▬ if no traffic is received because there are no frames where to check the FCS. It can

also indicate that the LED has been disabled due to the presence of a more important event.

Table 5.6: LED Indications

Metric	Description
REF	External clock input status LED. Displays green colour if a valid reference signal is found in the corresponding clock input port. Otherwise, the displayed LED colour is red.
LOCK	This LED is green when synchronization with the current clock has succeed. If external synchronization fails for some reason, the LED colour changes to red. Sometimes, it may take a few seconds to achieve synchronization with the external clock input. The LED colour during this transient period is yellow. The *LOCK* LED is enabled only when the clock reference is detected in the corresponding reference input clock interface.
10G	The port is operating at 10 Gb/s from the SFP+ port. Auto-negotiation is not defined in 10 Gb/s links and therefore this LED does not depend on any automatic process. It is enabled when a proper signal is detected in the SFP+ port input. The 10G LED is displayed only in Tempo units
1000	The port is operating at 1000 Mb/s either from the optical or the electrical port. Port speed is decided immediately after connecting the port to the DUT / SUT using Ethernet auto-negotiation or it is forced by the user.
100	The port is operating at 100 Mb/s from the electrical port. Port speed is decided immediately after connecting the port to the DUT / SUT using Ethernet auto-negotiation or it is forced by the user.
10	The port is operating at 10 Mb/s from the electrical port. Port speed is decided immediately after connecting the port to the DUT / SUT using Ethernet auto-negotiation or it is forced by the user.
RX	At least one frame was received during the current second in the current interface.

Table 5.6: LED Indications

Metric	Description
TX	At least one frame was transmitted during the current second in the current interface.
FCS	At least one frame with FCS errors has been found during the current second. A frame with a FCS error is a frame with a legal size which contains an invalid FCS field. FCS errors are caused by transmission errors. An optical Ethernet link with a poor power budget may experience FCS errors
Jabber	At least one jabber was received during the current second. Jabbers are defined as frames greater than 1518 bytes with a bad CRC.
UnderS	At least one undersized frame was received during the current second. An undersized frame is a frame which has a size smaller than 64 bytes.
OverS	At least one oversized frame was received during the current second. An oversized frame is a frame which has a size larger than the configured MTU.
VLAN	At least one frame with an VLAN tag was received during the current second in the current interface.
PB	At least one PB frame containing the IEEE 802.1ad Ethertype value (*0x88a8*) has been detected during the current second in the current interface. PB frames carry two VLAN tags known as S-VLAN and C-VLAN.
QinQ	At least one frame carrying two VLAN tags but not the IEEE 802.1ad Ethertype (*0x88a8*) has been detected during the current second in the current interface. Q-in-Q frames carry two VLAN tags known as S-VLAN and C-VLAN but they are not compliant with any international standard like the IEEE 802.1ad.

Table 5.6: LED Indications

Metric	Description
IP	If this led is green, at least one correct IPv4 or IPv6 datagram was received during the current second. If red, this led indicates that one incorrect datagram has been received during the current second. One IPv4 / IPv6 datagram is incorrect if its header has an unexpected structure, field values are different to the expected ones, it has an unexpected length or it contains checksum errors.
UDP	If this led is green, at least one correct UDP packet was received during the current second. If red, this led indicates that one incorrect datagram has been received during the current second. One UDP packet is incorrect if it has an unexpected length or it contains checksum errors.
TCP	If this led is green, at least one correct TCP packet was received during the current second. If red, this led indicates that one incorrect datagram has been received during the current second. One TCP packet is incorrect if it contains checksum errors.
LSS	Loss of Sequence Synchronization. This event indicates that the expected test pattern does not match the actually received test pattern. This event does not apply if the tester is configured to receive an SLA payload and, for framed analysis, it is referred to the stream 1 (the only stream with pattern analysis capabilities).
TSE	Test Sequence Error. One TSE is equivalent to a single bit difference between the transmitted and the received test pattern (PRBS or other). This event does not apply if the tester is configured to receive an SLA payload and, for framed analysis, it is referred to the stream 1 (the only stream with pattern analysis capabilities).

5.4. The Event Logger

Global counts, statistics and LEDs provide information about which events and how many of them have been registered but they do not say too much about how they are distributed in time. These information is supplied by the Tempo graphical representation tool or *event logger*.

With the Help of the event logger function, you can select one or various events and trace them so that all changes along with the time and date these changes are registered are recorded with a 1 second resolution. The event logger provides different representations and different zoom levels to enable event analysis at different time scales.

5.4.1. Configuring the Event Logger

Traceable Events are categorized in different classes. Moreover, each test port has its own traceable events. These events may be different for each test port.

Table 5.7: Logging event categories

Event class	Description
Anomalies / defects	Accounts for Ethernet /IPv4 /IPv6 anomalies and defects. This category includes the following events: *Link*, *FCS*, *Undersized*, *Oversized*, *Jabbers*, *IPv4 / IPv6 errors*, *UDP errors, TCP errors.*
Bandwidth statistics	Reports bit rates in *bit/s* for different protocol layers, including: *Ethernet bit rate*, *IPv4 bit rate*, *IPv6 bit rate*, *UDP bit rate*. The *Bandwidth statistics* category includes one set of traceable events for each filter (*Filter A1*, *Filter A2*,...) and one additional global statistics subclass.
Frame layer statistics	Event category that includes transmission statistics related with different frame structures: *RX frames*, *TX frames*, *Unicast*, *Multicast*, *Broadcast*, *VLAN*, *IEEE 802.1ad*, *Q-in-Q*, *Control*, *Pause*.
SLA statistics	Provides information about, delay, delay variation, frame loss and other QoS parameters. Includes the following events*: RX frames*, *RX bytes*, *FTD*, *FDV*, *Lost frames*, *Duplicated frames*, *SES*. This category has one subclass for each filter (*Filter A1*, *Filter A2,...*) so that metrics from different frame flows can be simultaneously traced and compared.
BERT	Reports BER results by means the *LSS*, *TSE* traceable events.
PTP	Includes events related with PTP performance in terms of latency, path asymmetry, PDV, time / frequency offset and wander. Traceable PTP events are: *Sync PTD (current)*, *Sync PDV (current)*, *Delay req. PTD (current)*, *Two-way PTD (current)*, *Sync IAD (current)*, *PTP slave frequency offset*, *PTP slave phase offset*, *Two way TE (Total)*, *Two way TE (Low freq.)*, *TE (High freq.)*, *Sync correction (current)*.

Table 5.7: Logging event categories

Event class	Description
Synchronization	This event category includes all events related with Synchronous Ethernet. Both message statistics, and time / frequency metrics are available. The traceable event list is: REF, OVF, TIE, Frequency offset, Frequency drift.
Reference events	*Sync loss*, *Visible satellites*, *Satellites used*, *PDOP*, *TDOP*

To enable the Event logger follow these steps.

1. From the *Home* panel, go to *TEST*,
   The *Test* configuration panel is displayed.
2. Select *Event logger setup*.
   The event logger configuration menu is displayed.
3. Enable event logging with the help of the *Enable* control.
4. Optionally, clear the currently selected filters with the *Clear all filters* menu.
5. Select the *Port A* or *Port B.*
6. Choose the event categories corresponding to the events you want to trace between: *Anomalies / defects*, *Bandwidth statistics*, *Frame layer statistics*, *SLA statistics*, *BERT*, *PTP*, *Synchronization*.
7. Select the events to be monitored from the category you have selected in the previous step.

Once event logging is enabled and the monitored events have been selected, the equipment starts generating one trace file for each test started with *Run* (or automatically through the Autostart/stop functionality).

5.4.2. Displaying Logs

You can either display trace files from finished tests or from the current test. You don't need to wait to the end of the test to display a trace file. To display the trace files and browse the events they contain follow this procedure:

1. From the *Home* panel, go to *RESULTS*,
   The *Results* panel is displayed.
2. Select *Event logger* to enter in event tracer.
3. Press the "..." button.
   A list with all the available trace files is displayed. Files are identified by the measurement start date and time. If there is an ongoing test, the name it is displayed with red characters.
4. Select one trace file and display it with the help of the *Open* control.
   A chronograph with the list of events included in the trace file is displayed. If the trace corresponding with an ongoing test is opened, then the unit shows the result evolution in real time and data is visualized as new results are collected.

5. Use the navigation bar on the bottom of the screen to browse the events recorded at different times. You can set the display scale to different zoom levels: *1 mins/ div, 5 mins/div*, *20 mins/div*, *1 hours/div*, *5 hours/div*, *20 hours/div, 2 days/div.*

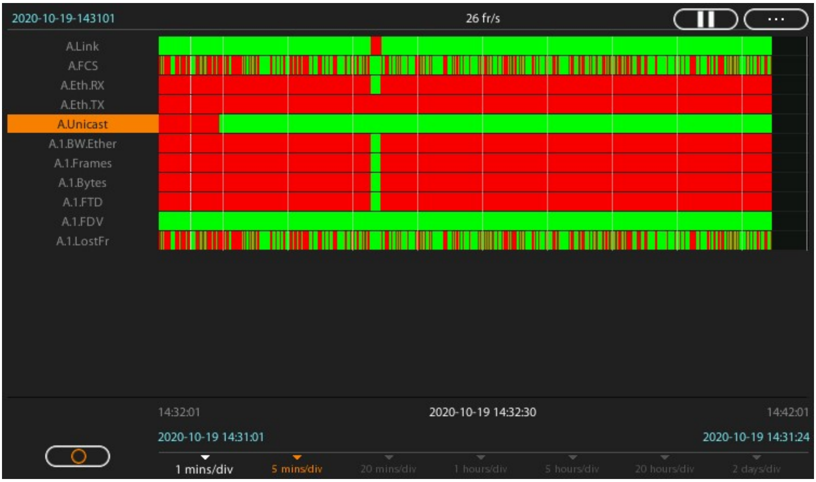


Figure 5.3: The Tempo event logger traces all events previously selected from the event filter.

6. Drag the plot to the left or the right to move through the time line.
Note: In ongoing tests it is necessary to first pause the plot by pressing the button located in the top left corner to enable the time line navigation. Once finished the test could be resumed with no data loss with the help of the same button.
7. Select an event in the list to and an instant in the time bar to display the magnitude of the event at the chosen time. Optionally, press again over the selected event to display detailed information about it, including a diagram of the amplitude for the current observation window.
8. Use the drag function in the detailed view in the same way that in the general chronograph plot. You can also use the auto scale, axis offset / resize and fast time axis navigation with the help of the keys located in the bottom left corner.

9. Press the back arrow to go back to the chronograph view of the plot.

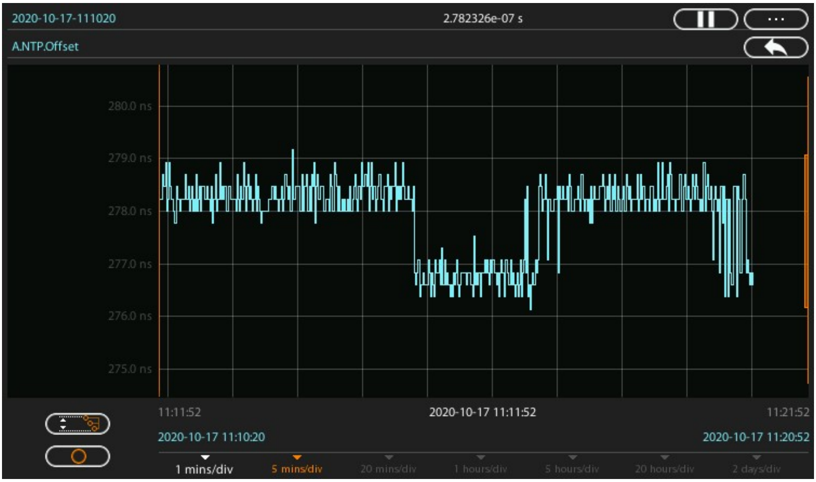


Figure 5.4: Tempo detailed view of events.

5.4.3. Exporting Logs

Users are allowed to export log files in CSV format. These files could be used as input for data processing software packages. A typical application is to use these graphics to generate high resolution plots from the data measured by Tempo. To export a file you can use the regular file exporting procedure for log files (See section 12.3.4). You can also export log files with the help of a web browser(See section 12.3.8).

Once the trace files have been exported to the external device they can be displayed, renamed or deleted form the file manager as any other output file generated by the test unit. (See section 12.3.2, See section 12.3.3). You can also copy and edit the log file to an external computer. Basically, a log file is a large table where each column corresponds with one event and each row is an instant of time. The table is filled with samples for the traced events collected at different instants of time.

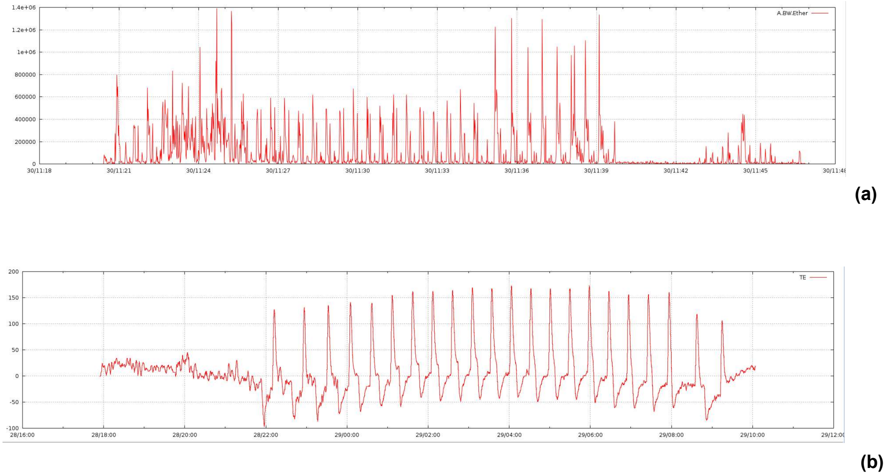


Figure 5.5: Plots generated from CSV files exported from Tempo: (a) Ether traffic plot from a web server, (b) Phase offset from a faulty network clock.

5.5. BER Testing

Tempo testers support Bit Error Rate (BER) testing over framed and unframed interfaces. The former computes the BER over Ethernet or IP interfaces, the later doesn’t take into account the frame structure associated to the Ethernet interface and accounts for bit errors directly in the physical layer.

5.5.1. Framed BER Tests

Framed BER tests are compatible with Ethernet and IP interfaces. It is even possible to carry out a BER test between specific source and destination UDP ports.

Framed BER test is not as useful in Ethernet as it is in TDM networks but it can be used to trace connectivity with remote equipments and detect any temporary availability fault. The tester considers that a frame contains bit errors when the test pattern carried by the frame does not match the expected pattern but the checksum fields are still correct. For this reason, Tempo Test Sequence Error (TSE) events are closer to corrupted frame events than to real transmission errors. In framed interfaces, transmission errors are likely to cause checksum errors and they are discarded before they can reach the test pattern analyser. In other words, for the tester, checksum errors (FCS errors, IPv4 errors, UDP errors, TCP errors) have higher precedence than bit errors. For this reason, transmission errors are usually accounted as a simultaneous checksum error and a lost frame event rather than a TSE event.

Tempo testers include one two test pattern generators and two pattern analysers, one for Port A and one for Port B. Pattern generator is bound with Flow 1 while traffic analysers are attached to Filter 1.

Table 5.8: BERT Results

Metric	Description
TSE	*Test Sequence Error*. One TSE is equivalent to a single bit difference between the transmitted and the received test pattern (PRBS or other). This field is a cumulative counter of all the TSE events found from the beginning of the test. In framed Ethernet interfaces transmission errors may cause the test patterns to be altered and produce bit errors. However, the Ethernet FCS field contains a CRC-32 code designed for error detection. For this reason, the receiver (or any intermediate network element) may detect and discard the frame before any TSE is detected by the pattern analyser. The only way to account for TSE errors would be to recompute the FCS field after any transmission error.
BER	The *Bit Error Ratio* (BER) this is the ratio of the received TSE to the total amount of transmitted bits. The BER is one of the most fundamental quality parameters of TDM digital circuits. However, due to other degradation sources specific of statistically multiplexed networks (frame loss, variable frame delay), the performance description based on the BER may be incomplete in Ethernet / IP networks.
ES	This is the amount of *Errored Second* (ES) outcomes from the beginning of the test. An ES is defined as a second which contains at least one TSE or a higher order defect like an LSS.
LSS	*Loss of Sequence Synchronization*. This event indicates that the expected test pattern does not match the actually received pattern. Frame loss events may cause temporary LSS.

Before running a framed BER test, first you need to make sure that your equipment is configured in *Ethernet endpoint* or *IP endpoint modes* (See section 2.1). The traffic generator must be configured in the same way than any other traffic test, including the physical layer settings, frame settings, the network settings and the bandwidth profile (See chapter 4). The procedure to configure the test is as follows:

1. From the *Home* panel, go to *CONFIG*,
   The test port settings panel is displayed.
2. Select either *Port A* or *Port B* to enter in the port specific configuration.
3. Enter in the *Payload* menu.
4. Select *Flow A1* (or *Flow B1* in *Port B*) to enter in the flow 1 specific configuration. All settings related with payload configuration in the current flow are displayed.
5. Choose one of *BERT* in *Payload type* (See section 4.1.4).
6. Choose the bit pattern you are going to use for generation and analysis with the help of the *BERT patterns* control.
7. If you have configured *BERT patterns* to *User*, enter a 32-bit test pattern in *User payload* in hexadecimal format.

Once the test has been configured it can be started at any time with the help of the *run* button. BER results for the last (or current) test are available at any time:

1. From the *Home* panel, go to *Results*,
   The test port results panel is displayed.
2. Select either *Port A or Port B* to enter in the port specific results.
3. Go to BERT
4. Select *Filter 1* to enter in the flow 1 specific results.
5. Check the *TSE BER*, *ES*, and *LSS* results.

5.5.2. Physical Layer BER Tests

The Physical Layer BER or L1 BER test measures the same parameters than the framed BER test but it is based on much simpler test patterns. Unlike the framed patterns, L1 patterns are fixed and not editable by the user. Some of them carry a minimum envelope like a preamble, an FCS or an IFG that enable some network elements to process the data stream in the same way than a framed flow. The advantage of L1 test patterns is that they are processed as a byte stream by the analyser (as opposed to a frame sequence). The result is a more accurate description of the transmission performance in terms of bit errors. On the other hand, L1 test patterns do not contain source and destination addresses or CoS labels to force the stream to follow an specific path in the network. Moreover, there is not a “bandwidth profile” you can use with L1 patterns, they are just byte sequences. At best, when they are carried within an Ethernet envelope, they use the whole capacity in the transmission interface.

The test unit supports three types of L1 test patterns referred as L1-unframed, L1-PCS-synchronized patterns and L2-compliant patterns. These are the properties of each type:

- *L1-unframed patterns:* They are constituted by a basic bit stream operating at the nominal speed defined for the interface. These patterns do not pass through network elements expecting an Ethernet stream but they are still useful to test the optical signal or data paths through L1 circuits not involving any Ethernet processing, even at the most basic level.

- *L1-PCS-synchronized patterns*: These patterns are defined by a sequence of *Physical Coding Sublayer* (PCS) symbols. For 1 Gb/s interfaces, L1-PCS-synchronized patterns are defined in terms of 8B/10B symbols. The pattern is not created as an 8-bit (8B) symbol and then converted to the correct 10-bit (10B) code. The result is that L1-PCS-synchronized patterns can be analysed at the bit level. L1-PCS-synchronized traffic passes through any circuit that has not any subsystem requiring valid MAC addressing or valid FCS codes.
- *L2-compliant patterns*: These test patterns are designed to resemble an Ethernet frame. The pattern is similar to a basic frame through de data link layer, including a preamble with a valid *Start of Frame Delimiter* (SFD), a FCS code and the correct encoding if the inter-frame gap. The pattern, however, overwrites all other parts of the frame, including MAC and IP addresses. L2-compliant patterns pass through any element looking for a valid Ethernet frame with FCS.

In Tempo, L1-PCS-synchronized patterns are supported only by the optical interfaces. L2-compliant patterns are available from all physical interface configurations.

Table 5.9: Test Patterns for Unframed Operation

Setting	Description
RPAT	*Random Data Pattern*. This is a L1-PCS-synchronized test pattern defined in the NCITS TR-25-1999. This pattern is designed to provide energy across the entire frequency spectrum, and they provide a good basic BER test. The RPAT consists on the continuous repetition of the following sequence expressed in hexadecimal format: 0x3e-b0-5c-67-85-d3-17-2c-a8-56-d8-4b-b6-a6-65. The RPAT is available for optical L1 BER tests only.
JPAT	*Jitter Tolerance Pattern*. This is a L1-PCS-synchronized test pattern defined in the NCITS TR-25-1999. This test is designed for receiver jitter tolerance testing. The JPAT consists on the cyclic transmission of the following 8B/10B symbol sequence: D30.3 (repeated 192 times) and D21.5 (repeated 64 times)

Table 5.9: Test Patterns for Unframed Operation

Setting	Description
SPAT	*Supply Noise test pattern*: This is a L1-PCS-synchronized test pattern defined in the NCITS TR-25-1999. It represents the worst-case power supply noise introduced by a transceiver. The SPAT consists on the cyclic transmission of the following hexadecimal pattern: 0xac-d4-ca-cd-4c (512 times). The SPAT is available for optical L1 BER tests only
HFPAT	*High Frequency test pattern*. This is a L1-PCS-synchronized test pattern defined in Annex 36A of the IEEE 802.3 standard. The purpose of the pattern is to test random jitter at a BER of 10^{-12}, and also to test the asymmetry of transition times. The HFPAT consists in the continuous repetition of the D21.5 code-group and it corresponds with the following bit sequence: 1010101010101010... The RPAT is available for optical L1 BER tests only.
LFPAT	*Low Frequency test pattern*. This is a L1-PCS-synchronized test pattern defined in Annex 36A of the IEEE 802.3 standard. The purpose of this pattern is to test low-frequency random jitter and also to test PLL tracking error. The LFPAT consists on the continuous repetition of the K28.7 code-group and it corresponds with the following bit sequence: 11111000001111100000... The RPAT is available for optical L1 BER tests only.
MFPAT	*Mixed Frequency test pattern*.This is a L1-PCS-synchronized test pattern defined in Annex 36A of the IEEE 802.3 standard. The purpose of this pattern is to test the combination of random and deterministic jitter. The MFPAT consists on the continuous repetition of the K.28.5 code-group and it corresponds with the following bit sequence: 11111010110000010100111110101 1... The RPAT is available for optical L1 BER tests only.

Table 5.9: Test Patterns for Unframed Operation

Setting	Description
LCRPAT	*Long Continuous Random test pattern*. This a L2-compliant test pattern defined in Annex 36A of the IEEE 802.3 standard. This pattern is designed to provide a broad spectral content and minimal peaking, allowing for the measurement of jitter at either the component or system level. The structure of the LCRPAT is based on cyclic transmission of a valid preamble, SDF sequence, the modified RPAT sequence repeated 126 times, a valid FCS and a 12-byte IFG The modified RPAT consists on the following sequence before the 8B/10B encoding: 0xbe-d7-23-47-6b-8f-b3-14-5e-fb-35-59.
SCRPAT	Sort Continuous Random test pattern. This is a L2-compliant test pattern defined in Annex 36A of the IEEE 802.3 standard. This pattern is designed to provide a broad spectral content and minimal peaking, allowing for the measurement of jitter at either the component or system level. The SCRPAT pattern structure is identical to the LCRPAT but the modified RPAT is repeated only 29 times resulting in shorter MAC frames.
A / B-Seed	This code is a L1-PCS-synchronized test pattern generated by loading predefined seeds *An*, *Bn*, *Ai*, *Bi* in an scrambler with polynomial $G(X) = 1 + X^{39} + X^{58}$ and predefined sequences at the scrambler input. The scrambler and the input is reset every 128 blocks (each block corresponds with a 64 bit code). As there are four seeds and four inputs, the pattern repeats every 512 blocks. The four seeds are defined as follows: • An: 0x3c-8b-44-dc-ab-68-04-f • Bn: 0x34-90-6b-b8-5a-38-88-4 • Ai: Results from bit wise inversion of An • Bi: Results from bit wise inversion of Bn The inputs are 0x00-00-00-00-00-00-00-00 (64-zeros), 0x55-00-00-01-00-00-00-01 (Local fault ordered set) and their inverted versions. The A/B-Seed pattern is available for 10 Gb/s interfaces only.

Table 5.9: Test Patterns for Unframed Operation

Setting	Description
PRBS 2^{31}-1	This code is a L1-unframed pattern corresponding with the output generated by a displacement register with polynomial $G(X) = 1 + X^{28} + X^{31}$.

The testers include two L1 test pattern generator and two pattern analysers (one for Port A and one for Port B). For a L1 BER test it is required one test pattern generator and at least one analyser. Generators and analysers can be physically located in one or various units. Configuration of L1 BER tests is slightly different than the L2-L4 framed BER test. The procedure is as follows:

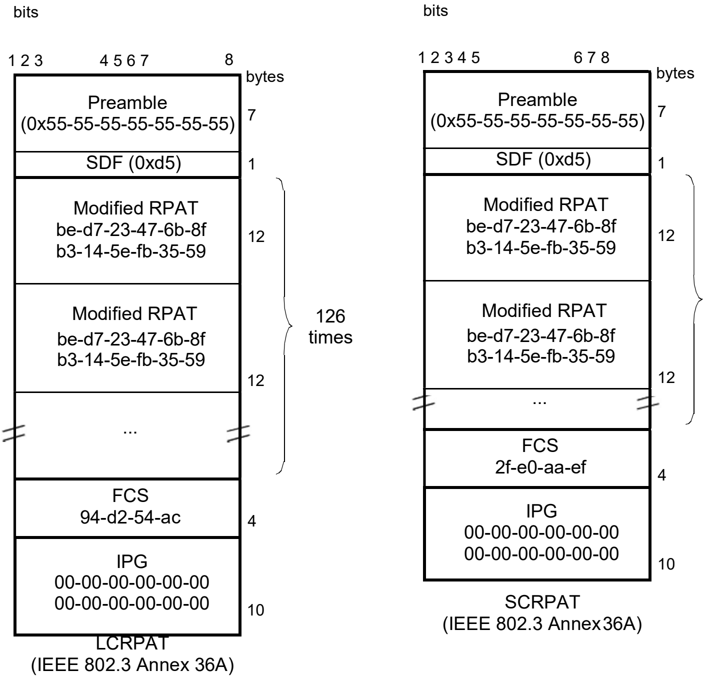


Figure 5.6: L2 compliant patterns supported by the Calnex family of Ethernet Generators / Analysers.

1. Make sure that your tester is connected to the network.
   Note: Depending on your test setup you may need to connect various equipments, including traffic reflectors in the network.
   Note: Testing with L1-PCS-synchronized patterns (optical tests) does not require link establishment. Pattern generation is started as soon as testing starts without waiting for link auto-negotiation or other link establishment mechanism to finish.

1. From the *Home* panel, go to *CONFIG*,
   The port configuration panel is displayed.
2. Select *Mode* to enter in the mode selection menu
3. Choose *L1 Endpoint*.
4. Select either *Port A* or *Port B* to enter in the port specific configuration.
5. Go to *L1 BERT pattern* and select one or *RPAT*, *JPAT*, *SPAT*, *HFPAT*, *LFPAT*, *MFPAT*, *LCRPAT*, *SCRPAT*, *A/B-Seed* or *PRBS* 2^{31}*-1*.
   Note: *RPAT*, *JPAT*, *SPAT*, *HFPAT*, *LFPAT*,*MFPAT, A/B-Seed and PRBS* 2^{31}*-1* patterns are not available in BER tests through electrical interfaces.
   Note: Depending on your particular test setup you may need to repeat this operation both Port A and Port B.

Once the test has been configured it can be started at any time with the help of the *run* button. BER results for the last (or current) test are available at any time:

1. From the *Home* panel, go to *RESULTS*,
   The test port results panel is displayed.
2. Select either *Port A or Port B* to enter in the port specific results.
3. Go to *BERT*
4. Select *Physical layer BERT* to enter in the L1 BER test results.
5. Check the *TSE, BER*, *ES*, and *LSS* results.

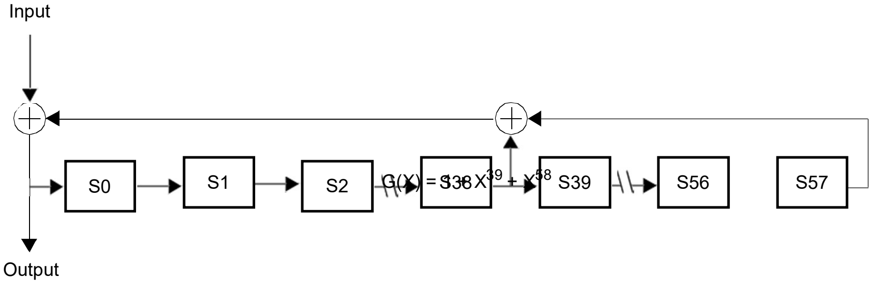


Figure 5.7: This diagram represents the scrambler required to generate the A-Seed and B-Seed patterns for 10 Gb/s LAN interfaces.

5.6. Service Disruption Time

The *Service Disruption Time* (SDT) test enables Tempo to find short Ethernet service interruptions.Some service disruptions are caused by problems that can be accounted for in time scales of seconds but some others, like the ones related with protection switching happen in time scales of milliseconds. The objective of the STD is to detect and report these short interruptions that could potentially last for a few milliseconds only.

Table 5.10: Service Disruption Time Results

Field	Description
Disruptions	Accounts for the number of times the service has been interrupted since the beginning of the test.
Total	Total amount of time the service has not been available due to disruptions. It is computed as the accumulated disruption tome from the beginning of the test.
Average	Average disruption time. This metric is computed as the value of the *Total* field divided by *Disruptions*.
Minimum	Shortest disruption time computed from the beginning of the test.
Maximum	Longest disruption time computed from the beginning of the test.
Last	Disruption time corresponding to the last disruption event computed by the test unit.

The SDT testing methodology requires the test unit to receive a constant bit rate of test frames. A warning message is displayed if the message rate is not large enough to achieve an accuracy level of 1 ms.The SDT is compatible both with *Ethernet endpoint* and *IP Endpoint* operation modes. To configure the SDT in your test unit you have to follow these steps:

1. Make sure that your tester is connected to the network. The physical layer must be up and working (See section 4.1.1) in all test ports to be used during the test.
2. Configure the test unit to generate al least 1000-frames/s (See section 4.1, See section 4.2).
   Note: The destination for the traffic could be *Port B* if traffic is generated from *Port A*, *Port A* if traffic is generated from *Port B* or a remote loopback device.
3. From the *Home* panel, go to *RESULTS*,
   The test port results panel is displayed.
4. Go to either Port A or *Port B, depending on where you are going to receive the test traffic you have configured previously.*
5. Go to *Service disruption time*.
6. Start the test by pressing *run*.
7. Check the *Disruptions*, *Total*, *Average*, *Minimum*, *Maximum* and *Last* results.
   Note: The accuracy in these results may not be the optimum if the test frame rate is below 1000 frames/s. In this case a *Measuring (low rate)* message is displayed in the results screen.

Chapter 6
Multi-Stream Analysis

Tempo is capable of processing and computing statistics over fractions of the Ethernet / IP traffic meeting specific conditions. The process of selecting a fraction of traffic is called filtering. The result of the filtering process is one or several traffic streams.

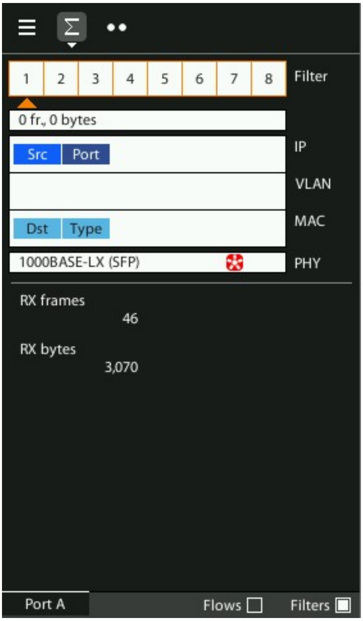
This chapter describes how to configure the tester for packet filtering and how to get statistics and results from each stream. These results can be classified in different categories:

- How many frames made up the traffic stream to be analysed. For example, filters can tell you how many frames have been received from an specific flow from the beginning of the test.
- The filter analysis tells what kind of data contains the traffic stream under analysis. For example, it the stream has at least some frames with the test payload required to measure SLA statistics you will be informed with an special indication.
- Filters are useful to get information about how much of the available bandwidth is being used by a traffic stream. If, for example, you choose to filter all broadcast IP packets (destination IPv4 address set to 255.255.255.255) you will measure how much traffic is consumed by broadcast traffic in your network like for example in ARP requests.
- Finally, the test unit provides per-filter information about critical SLA parameters like delay, delay variation or packet loss. It depends of the filtering criteria you are using that the SLA results you get are meaningful for your purposes ornot.

6.1. Enabling and Disabling Filters

Traffic selection or filtering is configured by first enabling one or several filtering blocks and after that setting the filtering criteria. Tempo supports Ethernet, VLAN, IPv4 and TCP / UDP filters.

The test unit is equipped with 8 filters per port (up to 16 filters in total). Each filter has a priority number. If one frame is selected by an specific filter it will not be processed by any lower priority filters. In other words, traffic is processed by at most one matching filter, the one with the highest precedence.



0 fr., 0 bytes

Src Port

Dst Type

1000BASE-LX (SFP)

RX frames 46

RX bytes 3,070

Figure 6.1: Filter summary panel. Filter status can be checked from this panel.

A filter admits three different configurations:

- *Block*: The filter blocks all the incoming traffic. No frame can match the filter. It can be considered that the filter remains disabled if it is configured to the block status.
- *Custom*: The filter accepts user defined matching rules like matching an specific VLAN, a group of source IP addresses and many others.
- *Match port A / Match port B*: Matches the traffic configured in the corresponding flow from the traffic generator (*Filter A1* matches *Flow A1*, *Filter A2* matches *Flow A2*, etc.). *The Match port A* mode is available for *Port B* only, while the *Match port B* is available for *Port A* only.
- *Match port A (loop) / Match port B (loop)*: Matches the traffic configured in the corresponding flow from the traffic generator (*Filter A1* matches *Flow A1*, *Filter A2* matches *Flow A2*, etc.). If this filtering mode is configured, the port expects that MAC addresses, IP addresses and UDP ports will be reversed when compared with the generator settings. For example, *Port A* looks for the IP address configured as a source in the IP destination address field of incoming traffic.*The Match*

port A (loop) mode is available for *Port A* only, while the *Match port B (loop)* is available for *Port B* only.

Current filtering configuration is always available from the summary screen. In this screen use the *Port A* and *Port B* contextual buttons to choose between Port A or Port B filters and the Filters check box to display filtering configuration.

6.2. Configuring Filters

To allow the filter to accept and process frames, a correct filtering criteria must be configured before being used. To configure the correct filtering criteria two decisions must be taken. First, it is necessary to know which frame fields are going to be matched and after that, which are the value or values to be matched. The first decision involves choosing whether the filtering is going to be done at MAC, IP or transport layer and which specific frame field or fields are going to be used for filtering (MAC addresses, IP addresses, Ethertype field, protocol or any other). The second is carried out by configuring the field value and sometimes a mask. The mask selects which field bits are taken into account when a frame is matched. Matching masks are not related to IP subnet masks even if they can be applied to IP addresses. Specifically, the binary representation of a matching mask does not need to be a sequence of '1' followed by a sequence of '0' like IP network masks are.

The generic procedure to configure one or several matching criteria in the test unit is the following:

1. From the *Home* panel, go to *CONFIG*,
   The test port settings panel is displayed.
2. Select either *Port A or Port B* to enter in the port specific configuration.
3. Enter in *Filters*
4. Select one of the filtering menus labelled as *Filter A1*, *Filter A2*, etc. (or *Filter B1*, *Filter B2*, etc. in *Port B*).
   All configuration items related with the filter configuration are displayed.
5. Configure Filter mode to one of *Block*, *Custom* or *Match port A / Match port B, Match port A (loop) / Match port B (loop)* values
   Block, Match port A / Match port B and *Match port A (loop) / Match port B (loop)* have fixed filtering rules but if you choose custom, different types of filtering rules are enabled for that filter: *Fixed offset*, *MAC*, C-*VLAN, S-VLAN, IPv4*, *IPv6, UDP*.
6. If you have configured *Custom* filtering, select the matching rule.
7. For custom filters, choose a matching field and configure the matching mode for this field. Most of the matching fields have at least two matching modes. The *Equal* mode selects frames matching the configured value or values for the field and *Ignore* does not match any frame by the current field. Other matching modes may be available in specific fields.
8. Configure the field value to be matched by the filter.

9. If the matching field has this capability, enter the mask value. To select a single value, set of the mask bit values to all ones.
10. Optionally, configure more matching rules for the current filter by repeating steps 3, 4, 5, 6, 7, 8 and 9 as many times as necessary.

6.2.1. MAC Selection

MAC frames are envelopes in which the Ethernet frames are sent and received. MAC frame format is currently specified by the standard IEEE 802.3. This format is shared by all existing Ethernet interfaces thus making Ethernet the most scalable transmission technology currently available.

Tempo provides frame selection based on the MAC address source and destination and Ethertype value. It is possible to configure a matching mask for all three fields to select a value set rather than a single value.

Table 6.1: MAC Selection

Field	Description
Source MAC address match	Enables selection by source MAC address in the current filter. The value configured here is used to determine which frames are allowed to pass through the filter and which ones are blocked. The available configuration values for this field are: • *Ignore*: The source MAC address is ignored and not taken into account for the purpose of the filter. No frame is selected by the filter when *Ignore* has been configured. • *Equal to*: All frames matching a user configurable pattern are allowed to pass through the filter. The matching pattern is configured with the help of the *Source MAC address* and *Source MAC address mask* fields.
Source MAC address	This is a 48-bit MAC address in the standard hexadecimal-digit format *XX:XX:XX:XX:XX:XX*. Source addresses matching some or all bits of the address configured here will be allowed to pass through the filter. Bits used for matching frames to this filter are configured in the *Source MAC address mask*.
Source MAC address mask	This is the mask for the source MAC address filter selection rule. Before comparing the *Source MAC address* field with the frame addresses, bit wise AND operations are carried out between the value configured here and the *Source MAC address* field so that only the values surviving the AND are taken into account for matching the filter.

Table 6.1: MAC Selection

Field	Description
Destination MAC address match	Enables selection by destination MAC address in the current filter. The value configured here is used to determine which frames are allowed to pass through the filter and which ones are blocked. The available configuration values for this field are the same that for the *Source MAC address selection* setting.
Destination MAC address	This is a 48-bit MAC address in the standard hexadecimal-digit format *XX:XX:XX:XX:XX:XX*. Destination addresses matching some or all bits of the address configured here will be allowed to pass through the filter. Bits used for matching frames to this filter are configured in the *Destination MAC address mask*.
Destination MAC address mask	This is the mask for the destination MAC address filter selection rule. Before comparing the *Destination address* field with the frame addresses, bit wise AND operations are carried out between the value configured here and the *Destination address* field so that only the values surviving the AND are taken into account for matching the filter.
Ethertype match	Enables selection by Ethertype value in the current filter. The value configured here is used to determine which frames are allowed to pass through the filter and which ones are blocked. The available configuration values for this field are the same that for the *Source address selection* and *Destination address selection* settings.
Ethertype	This setting contains a 2-byte field that constitutes the Ethertype value to be matched in the incoming traffic. Ethertypes matching some or all bytes of the value configured here will be allowed to pass through the filter. Bits used for matching frames to this filter are configured by means the *Ethertype mask*.
Ethertype mask	This is the mask for the Ethertype filter selection rule. Before comparing the *Ethertype* field with the frame Ethertype, bit wise AND operations are carried out between the value configured here and the *Ethertype* field so that only the values surviving the AND are taken into account for matching the filter.

6.2.2. C-VLAN and S-VLAN Selection

Within enterprise networks, VLANs are important because they enable network segmentation on an organisational basis, by functions, project teams or applications, rather than on a physical or a geographical basis. The network can be reconfigured through software, instead of physically unplugging and moving devices or wires.

VLANs are an important contribution to scalable Ethernet networks, because they limit broadcast traffic inherent to the bridging mechanism. Large amounts of broadcast traffic may damage performance and even collapse network equipment, which is why it must be controlled.

Standard IEEE 802.1Q specifies the most popular VLAN frame format. VLAN frames carry a 16-bit header which specifies the VLAN Identifier (VID) and the frame priority within the VLAN. Many carrier Ethernet networks use the VID for segmentation just like enterprises. The VID in carrier Ethernet networks is used by service providers as general purpose identifier. They can be associated to an specific service, customer, node or several of them at the same time. Sometimes, service providers use a two-level VLAN structure. Levels are designated as customer VLAN (C-VLAN) and service VLAN (S-VLAN). This two-structure is know as Q-in-Q. The standardised version of the Q-in-Q frame is defined in IEEE 802.1ad. The test unit supports both single-level Q-frame and the two-level Q-in-Q-frame.

Table 6.2: C-VLAN and S-VLAN Selection

Field	Description
VID match	Enables selection by VID in the current filter. The value configured here is used to determine which frames are allowed to pass through the filter and which ones are blocked. The available configuration values for this field are: • *Ignore*: The VID is ignored and not taken into account for the purpose of the filter. No frame is selected by the filter when *Ignore* has been configured. • *Equal to*: All frames matching a user configurable pattern are allowed to pass through the filter. The matching pattern is configured with the help of the *VID* field.
VID	This setting contains a 10-bit identifier that constitutes the VID value to be matched in the incoming traffic. It is possible to match the S-VID or the C-VID through separated entries in the filtering menu. For single-tagged frames it is assumed that the frame does not contain S-VID field and therefore configuration is done through the C-VLAN menu.

Table 6.2: C-VLAN and S-VLAN Selection

Field	Description
Priority codepoint match	Enables selection by IEEE 802.1Q/p priority bits in the current filter. The value configured here is used to determine which frames are allowed to pass through the filter and which ones are blocked. The available configuration values for this field are the same that for the *VID match* field.
Priority codepoint	This setting contains a 3-bit identifier that constitutes the priority value to be matched in the incoming traffic. It is possible to match the S-VLAN or the C-VLAN priority codepoints through separated entries in the filtering menu. For single-tagged frames it is assumed that the frame does not contain S-VLAN priority codepoint field and therefore configuration is done through the C-VLAN menu.
Drop-eligible indicator match	Enables selection by the S-VLAN drop-eligible indicator in the current filter. The value configured here is used to determine which frames are allowed to pass through the filter and with ones are blocked. The available configuration values for this field are the same that for the *VID match* field.
Drop-eligible indicator	This is a single bit field that is used to signal which frames have precedence when the node has to drop some information due to congestion or other causes. The Drop-eligible indicator is defined only for the S-VLAN tag of double-tagged frames.For this reason is only available for S-VLAN matching rules.

6.2.3. MPLS Selection

MPLS traffic carry one or various 4-byte headers. Each of these headers is made up of a 20-bit MPLS label, a 3-bit traffic class identifier and other fields (See section 4.2.2).

The filtering capabilities of the test unit can be used to match MPLS header field of IP packets carrying up to two different labels.

Table 6.3: MPLS Selection

Field	Description
Bottom label match	Enables selection based on the bottom MPLS label in the current filter. The value configured here is used to determine which frames are allowed to pass through the filter and which ones are blocked. The available configuration values for this field are: • *Ignore*: The bottom MPLS label is ignored and not taken into account for the purpose of the filter. No frame is selected by the filter when *Ignore* has been configured. • *Equal to*: All frames matching a user configurable MPLS label are allowed to pass through the filter. This label is configured with the help of the *Bottom label* field.
Bottom label	Bottom of the stack MPLS label. It is 20-bit MPLS label in decimal format. Labels are used for switching packets in MPLS networks. Labels have local meaning only. That means that a single LSP could have different MPLS labels in different links between different routers
Bottom traffic class match	Enables selection based on the class of service bits included in the top MPLS label in the current filter. The value configured here is used to determine which frames are allowed to pass through the filter and which ones are blocked. The available configuration values for this field are: • *Ignore*: The bottom class of service field is ignored and not taken into account for the purpose of the filter. No frame is selected by the filter when *Ignore* has been configured. • *Equal to*: All frames matching a user configurable class of service field are allowed to pass through the filter. The class of service field is configured with the help of the *Bottom traffic class* field.
Bottom traffic class	Bottom 3-bit MPLS CoS identifier. It was first thought that this field could carry the 3 IPv4 Type-of-Service (ToS) bits, but currently, the ToS field is being replaced by 6-bit *Differentiated Services Code Points* (DSCP). This means that only a partial mapping of all the possible DSCPs into this field is possible.

Table 6.3: MPLS Selection

Field	Description
Top label match	Enables selection based on the top MPLS label in the current filter. Top label matching makes sense only if the received packets carry two MPLS labels. In this case the top label is the one placed closer to the layer two header. The available configuration values for this field are the same that for the *Bottom label match* setting.
Top label	Top of the stack MPLS label. It is 20-bit MPLS label in decimal format. Labels are used for switching packets in MPLS networks. Labels have local meaning only. That means that a single LSP could have different MPLS labels in different links between different routers
Top traffic class match	Enables selection based on the class of service bits included in the top MPLS label in the current filter. The available configuration values for this field are the same that for the *Top label match* setting.
Top traffic class	Top 3-bit MPLS CoS identifier. It was first thought that this field could carry the 3 IPv4 Type-of-Service (ToS) bits, but currently, the ToS field is being replaced by 6-bit *Differentiated Services Code Points* (DSCP). This means that only a partial mapping of all the possible DSCPs into this field is possible.

6.2.4. IPv4 Selection

The test unit filtering capabilities can be programmed to match fields within the IPv4 datagram. It is currently supported IP datagram matching based on source IP address, destination IP address, protocol and DSCP. Source and destination IP addresses can be matched by means selection masks.

Table 6.4: IPv4 Selection

Field	Description
Source IPv4 address match	Enables selection by source IPv4 address in the current filter. The value configured here is used to determine which frames are allowed to pass through the filter and which ones are blocked. The available configuration values for this field are: • *Ignore*: The source IP address is ignored and not taken into account for the purpose of the filter. No frame is selected by the filter when *Ignore* has been configured. • *Equal to*: All frames matching a user configurable pattern are allowed to pass through the filter. The matching pattern is configured with the help of the *Source IPv4 address* and *Source IPv4 address mask* fields.
Source IPv4 address	This is a 32-bit IPv4 address in the standard four-dotted decimal format *A.B.C.D*. Source addresses matching some or all bits of the address configured here will be allowed to pass through the filter. Bits used for matching frames to this filter are configured in the *Source address mask*.
Source IPv4 address mask	This is the mask for the source IPv4 address filter selection rule. Before comparing the *Source address* field with the frame addresses, bit wise AND operations are carried out between the value configured here and the *Source address* field so that only the values surviving the AND are taken into account for matching the filter.
Destination IPv4 address match	Enables selection by destination IPv4 address in the current filter. The value configured here is used to determine which frames are allowed to pass through the filter and which ones are blocked. The available configuration values for this field are the same that for the *Source IPv4 address match* setting.
Destination IPv4 address	This is a 32-bit IPv4 address in the standard four-dotted decimal format *A.B.C.D*. Destination addresses matching some or all bits of the address configured here will be allowed to pass through the filter. Bits used for matching frames to this filter are configured in the *Destination address mask*.

Table 6.4: IPv4 Selection

Field	Description
Destination IPv4 address mask	This is the mask for the source IPv4 address filter selection criteria. Before comparing the *Source address* field with the frame addresses, bit wise AND operations are carried out between the value configured here and the *Source address* field so that only the values surviving the AND are taken into account for matching the filter.
IP protocol match	Enables selection by the 1-byte IPv4 protocol field in the current filter. The value configured here is used to determine which frames are allowed to pass through the filter and which ones are blocked. The available configuration values for this field are the same that for the *Source IPv4 address match* setting.
IP protocol	Configures the protocol to be filtered when protocol selection is enabled. The available configuration values are the following: • *Numeric*: Use this control if the traffic to be matched is different of UDP, TCP and ICMP and it has an specific protocol identifier assigned by the IANA. • *UDP*: Matches traffic with a *User Datagram Protocol (UDP)* envelope. Traffic commonly transported over UDP includes IP voice, IP video and DNS. • *TCP*: Matches traffic carried over the Transfer Control Protocol (TCP). Most data applications (web, file transfer, e-mail...) ere normally based on TCP transport. • *ICMP*: Matches *Internet Control Message Protocol* packets. IP operation and maintenance traffic like ping use ICMP.
IP protocol number	This setting contains an 8-bit word that constitutes the protocol identifier to be matched in the incoming traffic. Configuring this field to 17 is equivalent of setting the *Standard protocol selection* to UDP. TCP uses 6 as the protocol number and ICMP uses number 1. This control is enabled only if Standard protocol selection has been previously set to *Numeric*.
DSCP match	Enables selection by the 6-bit DSCP field in the current filter. The value configured here is used to determine which frames are allowed to pass through the filter and which ones are blocked. The available configuration values for this field are the same that for the *Source IPv4 address match* field.

Table 6.4: IPv4 Selection

Field	Description
DSCP	This setting contains a 6-bit word in decimal format that constitutes the DSCP to be matched in the incoming traffic.

6.2.5. IPv6 Selection

Version 6 of the IP protocol is increasingly important in current network deployments. For this reason, the test unit supports filtering based on various IPv6 packet fields including addresses, CoS marks, flow labels and higher layer protocol identifiers.

Table 6.5: IPv6 Selection

Field	Description
Source IPv6 address match	Enables selection by source IPv6 address in the current filter. The value configured here is used to determine which packets are allowed to pass through the filter and which ones are blocked. The available configuration values for this field are: • *Ignore*: The source IP address is ignored and not taken into account for the purpose of the filter. All packets are allowed to pass through the filter when *Ignore* is configured if they are not blocked by other selection rule. • *Equal to*: All packets matching a user configurable pattern are allowed to pass through the filter. The matching pattern is configured with the help of the *Source IPv6 address* and *Source IPv6 address mask* objects.
Source IPv6 address	This is a 128-bit IPv6 address in the *A:B:C:D:E:F:G:H* format, where *A*, *B*, *C*, *D*, *E*, *F*, *G* and *H* are hexadecimal numbers between *0000* and *ffff*. Source addresses matching some or all bits of the address configured here will be allowed to pass through the filter. Bits used for matching packets to this filter are configured by means the *Source IPv6 address mask* field.
Source IPv6 address mask	This is the mask for the source IPv6 address filter selection rule. Before comparing the *Source IPv6 Address Match* field with the actual IPv6 addresses, bit wise *AND* operations are carried out between the value configured here and the source address so that only the values surviving the *AND* are taken into account for matching addresses.

Table 6.5: IPv6 Selection

Field	Description
Destination IPv6 address match	Enables selection by destination IPv6 address in the current filter. The value configured here is used to determine which frames are allowed to pass through the filter and which ones are blocked. The available configuration values for this field are the same that for the *Source IPv6 address match* setting.
Destination IPv6 address	This is a 128-bit IPv6 address in the *A:B:C:D:E:F:G:H* format, where *A*, *B*, *C*, *D*, *E*, *F*, *G* and *H* are hexadecimal numbers between *0000* and *ffff*. Destination addresses matching some or all bits of the address configured here will be allowed to pass through the filter. Bits used for matching packets to this filter are configured by means the *Destination IPv6 address mask* field.
Destination IPv6 address mask	This is the mask for the destination IPv6 address filter selection rule. Before comparing the *Destination IPv6 Address Match* field with the actual IPv6 addresses, bit wise *AND* operations are carried out between the value configured here and the source address so that only the values surviving the *AND* are taken into account for matching addresses.
Next Header match	Enables selection by the 8-bit IPv6 next header field in the current filter. The value configured here is used to determine which packets are allowed to pass through the filter and which ones are blocked. The available configuration values for this field are the same that for the *Source IPv6 address match* setting.
Next Header	Configures the protocol identifier to be filtered when *Next Header matching* is enabled. The available configuration values are the following: • *Numeric*: Use this control if the traffic to be matched is different of UDP, TCP and ICMP and it has an specific protocol identifier assigned by the IANA. • *UDP*: Matches traffic with a *User Datagram Protocol (UDP)* envelope. Traffic commonly transported over UDP includes IP voice, IP video and DNS. • *TCP*: Matches traffic carried over the Transfer Control Protocol (TCP). Most data applications (web, file transfer, e-mail...) ere normally based on TCP transport. • *ICMP*: Matches *Internet Control Message Protocol* packets. IP operation and maintenance traffic like ping use ICMP.

Table 6.5: IPv6 Selection

Field	Description
Next Header number	This object contains an 8-bit word that constitutes the next header identifier to be matched in the incoming traffic. For example, configuring this object to 17 matches UDP traffic, TCP uses 6 as the protocol number and ICMPv6 uses number 58. The *Next Header number* configuration field is enabled only if *Next Header* is configured to *Numeric*.
Flow Label match	Enables selection by the 20-bit IPv6 flow label field in the current filter. The value configured here is used to determine which packets are allowed to pass through the filter and which ones are blocked. The available configuration values for this field are the same that for the *Source IPv6 address match* setting.
Flow label	The *Flow Label* IPv6 field contains a 20-bit word that identifies an unidirectional data flow. These labels remain at disposal of intermediate routers for stateful and stateless processing at flow level. For example, the flow label could be used to prevent load balancing on a particular traffic flow.
DSCP match	Enables selection by the 6-bit differentiated services code point (DSCP) field in the current filter. The value configured here is used to determine which packets are allowed to pass through the filter and which ones are blocked. The available configuration values for this field are the same that for the *Source IPv6 address match* field.
DSCP	This object contains a 6-bit word in decimal format that constitutes the DSCP to be matched in the incoming traffic.

6.2.6. UDP Selection

Some applications do not require reliable transmission at the transport layer either because they implement their own error control mechanisms or because the mechanisms used by TCP are too slow for them. These applications can use the light weight User Datagram Protocol (UDP). Like TCP, UDP provides communications through ports to applications but it doesn't have any error recovery capability.

Table 6.6: UDP Selection

Field	Description
Source port match	Enables selection by source UCP port in the current filter. The value configured here is used to determine which frames are allowed to pass through the filter and which ones are blocked. The available configuration values for this field are: • *Ignore*: The source port is ignored and not taken into account for the purpose of the filter. No frame is selected by the filter when *Ignore* has been configured. • *Range*: All frames with a destination port in an specified range are allowed to pass through the filter. The port range is specified with the help of the *Minimum source port* and *Maximum source port* fields.
Minimum source port	This is the minimum 16-bit UDP source port allowed to pass through the *Source port match* filter. The port is configured and displayed in decimal format.
Maximum source port	This is the maximum 16-bit UDP source port allowed to pass through the *Source port match* filter. The port is configured and displayed in decimal format.
Destination port match	Enables selection by the 2-byte UDP protocol field in the current filter. The value configured here is used to determine which frames are allowed to pass through the filter and which ones are blocked. The available configuration values for this field are the same that for the *Source address match* field.
Minimum destination port	This is the minimum 16-bit UDP destination port allowed to pass through the Destination port selection filter. The port is configured and displayed in decimal format.
Maximum destination port	This is the maximum 16-bit UDP destination port allowed to pass through the Destination port selection filter. The port is configured and displayed in decimal format.

6.2.7. TCP Selection

Th e Transfer Control Protocol (TCP) provides reliable, connection oriented, transmission of information thanks to a sophisticated error detection and frame retransmission mechanism. It also includes flow control, congestion avoidance and other features to improve protocol reliability. Due to these functions, TCP is suitable for data applications such as file transfer, web browsing and e-mail.

TCP applications identify themselves though a 16-bit port both at the data source and sink. From this point of view, TCP is similar to UDP. The Tempo TCP protocol filter function enables users to select specific source and destination ports or port ranges. Configuration follows exactly the same procedure than in UDP.

6.2.8. Protocol Selection

The protocol selection is useful when filtering over layer four is required. Protocol selection us useful when used together with other functions such as the IEC 68150 analysis (See section 11.3) or the traffic capture function (See section 6.4). Protocols currently supported are PTP, NTP, GOOSE and SV.

Table 6.7: Protocol Selection

Field	Description
Protocol	Enables selection by protocol in the current filter. The value configured here is used to determine which frames are allowed to pass though the filter ans which ones are blocked. The available configuration values are: • *Ignore*: Protocol matching is ignored and not taken into account for the purpose of the filter. All frames are allowed to pass though the filter when Ignore is configured if they are not blocked by the other selection criteria. • *PTP*: Matches frames carrying *Precision Time Protocol* messages. The exact structure and content matched by the filter are determined with the help of the *Transport protocol*, *Message type match* and *Domain match* fields • *NTP*: Matches messages from the *Network Time Protocol* (NTP). The exact structure and content of the frames matched by this filter is determined by the *Message direction* and *Message type match*. • *GOOSE*: Matches *Generic Object Oriented Substation Events* (GOOSE) protocol messages. Users can optionally specify an application ID for the filtered GOOSE messages through the *Application ID match* setting. • *SV*: Matches *Samples Values* (SV) protocol messages. Users can optionally filter traffic from an specific application ID through the *Application ID match* field.
Transport protocol	If PTP protocol filtering is configured, this setting allows users to set the frame structure of the messages to be filtered. It can be either Ethernet or UDP (See section 9.1.4).

Table 6.7: Protocol Selection

Field	Description
Message type match	With PTP or NTP filtering, it selects the message type to be filtered. This field could be configured to any of the following values: • *Ignore*: Message type matching is ignored and nottaken into account for the purpose of the filter. All frames are allowed to pass through the filter when *Ignore* is configured if they are not blocked by other selection criteria. • *Equal to*:All frames matching the NTP or PTP message type configured through the *Message type* field are allowed to pass through the filter.
Message type	This field configures the PTP or NTP message type to be matched. In PTP filters it is any of *Sync*, *Delay Request*, *Delay Response*, *Peer Delay Request*, *Peer Delay Response*, *Follow-up*, *Peer Delay Follow-up*, *Announce*, *Signaling*, *Management*. In NTP filters, this field could be configured to *Symmetric Active*, *Symmetric Passive*, *Client*, *Server*, *Broadcast*, *Control* and *Other*.
Domain match	With PTP filtering, it selects the PTP domain number to be filtered. This field can be configured to any of the following values: • *Ignore*: Domain matching is ignored and not taken into account for the purpose of the filter. All frames are allowed to pass through the filter when *Ignore* is configured if they are not blocked by other selection criteria. • *Equal to*:All frames matching the NTP or PTP message type configured through the *Message type* field are allowed to pass through the filter.
Domain	If domain matching is enabled, this setting configures the PTP domain (a number between 0 and 255) to be matched by the filter. Only frames matching the domain configured here are allowed to pass though the filter.
Message direction	In NTP filtering mode, it configured the message direction to be matched. It could be *From server* or *To server*.

Table 6.7: Protocol Selection

Field	Description
Application ID match	In GOOSE or SV filtering modes, it enable the user to select an specific application ID to select frames. This field can be configured to any of the following values: • *Ignore*: Domain matching is ignored and not taken into account for the purpose of the filter. All frames are allowed to pass through the filter when *Ignore* is configured if they are not blocked by other selection criteria. • *Equal to*: All frames matching the NTP or PTP message type configured through the *Message type* field are allowed to pass through the filter.
Application ID	If filtering by application ID is configured, then this field configured the specific value of the ID to be filtered.

6.2.9. Fixed Offset Selection

Generic selection is the matching mode to be used when the Ethernet frames carry uncommon protocols or if inspection beyond the UDP and TCP transport protocols is required. This selection mode defines an offset and a mask. Frames matching the specified mask in the configured offset are selected.

Table 6.8: Generic Selection

Field	Description
Filter match	Enables fixed offset selection in the current filter. The value configured here is used to determine which frames are allowed to pass through the filter and which ones are blocked. The available configuration values for this field are: • *Ignore*: Generic matching is ignored and not taken into account for the purpose of the filter. All frames are allowed to pass through the filter when *Ignore* is configured if they are not blocked by other selection criteria. • *Equal to*: All frames matching a user configurable pattern are allowed to pass through the filter. The matching pattern is configured with the help of the *Payload selection*, *Offset (bytes)*, *Match code* and *Mask* fields.

Table 6.8: Generic Selection

Field	Description
Payload selection	Defines the payload type and the reference point within the frame to start counting the filter offset. The reference can be the beginning of the MAC, IPv4, IPv6 or UDP payload depending on the chosen value. It is also possible to set the reference to the beginning of the Ethernet frame (first byte immediately after the SDF) by configuring *Whole frame* in this field. The *Payload selection* field is shared by all the port A or port B filters. If the *Frame start* field is modified for one specific filter, the remaining filters of the same port will be automatically configured to the same value.
Offset (bytes)	This field defines the offset expressed in bytes from the reference point defined with the *Payload selection* control. The value 0 corresponds with the first byte of the MAC, IPv4 or UDP payload (or the first frame byte, if *Payload selection* is set to *Whole frame*). If due to the limited frame size, some or all the byte positions defined by the *Offset (bytes)* field, do not exist in the corresponding payload, the equipment will consider that the frame does not match the filtering criteria. The offset field is shared by all the port A or port B filters. If the *Offset (bytes)* field is modified for one specific filter, the remaining filters of the same port will be set to the same value.
Match code	16-bit code expressed with four hexadecimal digits used to match frames.in the current filter.
Mask	This is a mask for the generic filter match code. Before comparing the *Match code* with the selected bytes in the Ethernet frame, bit wise AND operations are carried out between the value configured here and the *Match code* field so that only the values surviving the AND are taken into account for matching the filter.

6.3. Per-Stream Counts and Statistics

Once the filter has been configured, it is usually desirable to know how many matching frames have been found for each filter and what are the matching traffic properties. Tempo offers a complete set of statistics for each of the eight filtered streams, including bandwidth and SLA metrics. To get general statistics about filtered frames follow this procedure:

1. From the *Home* panel, go to *RESULTS*,
   The test port results panel is displayed.
2. Select either *Port A or Port B* to enter in the port specific results.
3. Go to *Filters*
   A table with dedicated information for each filter is displayed.
4. Check the *Frames*, *Bytes* and *Traffic* results.

Table 6.9: General Filter statistics

Field	Description
Frames	Count of all frames matching the selection rule for the current filter.
Bytes	Byte count corresponding to the traffic stream associated with the current filter. Note that only with the *Frames* and *Bytes* results it is possible to compute new statistics like the average frame size of the matching traffic.
Traffic	Displays information about the traffic type detected during the last second. There are three possible results: • *None*: No traffic has been detected matching the filtering rules for the current filter during the last second. Either there is no traffic received in the port or the filter rules are too restricting to match any frame. • *Other*: At least one frame of network traffic matching the filter rules has been found during the last second. Traffic may come from anywhere in the network. • *SLA*: At least one frame carrying the Calnex SLA payload and matching the filter rules has been found during the last second. The SLA payload is Calnex pro- prietary and therefore it has probably been transmitted by an Calnex equipment. SLA statistics for the current filter cannot be calculated if no SLA traffic match- ing the filtering rules is received.

6.3.1. Bandwidth Statistics

Filter specific bandwidth statistics have the same meaning that the port-wide bandwidth statistics (See section 5.1.4) but in this case they are restricted to the traffic matching the filtering rules rather than the whole traffic received in the test port. Let’s suppose that you want to know how much bandwidth is using an IPTV stream in your network. If you know some information about the stream like for example the destination UDP port used by the stream packets or the destination multicast IP address you can use them as a filtering rules and the bandwidth statistics for the filtered traffic will provide the result in the Ethernet, IP and UDP layers.

The procedure to display the bandwidth statistics for each of the configured filters is as follows:

1. From the *Home* panel, go to *RESULTS*,
   The test port results panel is displayed.
2. Select either *Port A or Port B* to enter in the port specific results.
3. Go to *Bandwidth statistics.*
4. Select one of the filter menus labelled as *Filter A1*, *Filter A2*, etc. (or *Filter B1*, *Filter B2*, etc in Port B).
   All the result menus related with the current filter are displayed.
5. Check the *Eth. (current)*, *Eth. (min.)*, *Eth (max.)*, *IPv4 (current)*, *UDP (current)* results.

6.3.2. SLA Statistics

SLA statistics are more similar to BER results than bandwidth statistics or error counts: Like it happens with BER results, SLA statistics require an special frame / packet payload. In this case, the payload to be used is the SLA payload (See section 4.1.4, See section 4.2.6). That means that the tester you are using as a traffic generator must be configured to use this payload to obtain any valid result.

Table 6.10: SLA Availability Statistics

Field	Description
Lost frames	Total amount of lost frames from the beginning of the test. One frame is considered to be lost if it is never received or if it is received with a delay larger than 10 seconds.
FLR	Ratio of the total amount of lost frames to the total transmitted frames from the beginning of the test. Definition of the FLR parameter follows ITU-T Y.1563.
SES	This is the amount of Severely Errored Second (SES) outcomes from the beginning of the test. The SES is computed as specified in ITU-T Y.1563. The frame loss threshold used to declare a SES is 50% of the frames that made up the transmitted block.
PEU (%)	Percent Ethernet service Unavailability defined as per ITU-T Y.1563 and recorded from the beginning of the test. The PEU constitutes a availability performance figure that informs about the percentage of time that the DUT / SUT has been not available for transmit / receive data.

Table 6.10: SLA Availability Statistics

Field	Description
Out-of-sequence frames	Total amount of packets received with an unexpected sequence number. Duplicated sequence numbers are not taken into account for computing the Out-of-sequence frame statistic. This metric is based on the definitions given in RFC 5236.
Duplicated frames	Total amount of frames received with a duplicated sequence number. A triplicated frame event is accounted as two duplicated frame events. The same reasoning is applied for frames repeated more than three times. The duplicated frames metric is based on the definitions given in RFC 5236.

It is possible to use the same test port for SLA traffic generation and analysis (Port A) or use Port A for traffic generation and Port B for analysis. Using Port A for generation and analysis requires a loop-back device somewhere in the network to redirect the traffic towards the origin (See section 2.2.3). It is also possible to generate traffic with one tester and use a remote equipment to analyse this traffic but delay statistics will be probably wrong or at least will have a poor accuracy due to the lack of a common timing source for the generator and the analyser.

The test unit supports SLA tests both in bridged environments (*Ethernet endpoint* test mode) and routed environments (*IP endpoint* test mode). Traffic generation in pass through mode is not supported, for this reason, there are no SLA results in *IP Through* mode.

The testers measure and represent up to eight sets of SLA statistics per test port for each of the eight filter blocks. An important advise is that strictly, SLA results are meaningful only for frames carrying the SLA payload. Other traffic accounted in the same filter may be subject to different delay conditions. However, if one filter is receiving mixed (SLA and not SLA) traffic, it is possible to guarantee the representativeness of the SLA results if the correct filtering conditions are applied for the traffic. For example if it is know that the DUT / SUT is applying different forwarding policies depending only on the DSCP field, filters should be configured to use the DSCP as a filtering rule.

SLA results are timed, you need to start a test with *run* to enable the equipment to collect results. If you are using the equipment also as a test traffic generator you will also need to start a test to enable traffic generation. Once the test is configured and running you can access to the results. To configure and run an SLA test follow these steps:

1. From the *Home* panel, go to *RESULTS*,
   The test port results panel is displayed.

2. Select either *Port A or Port B* to enter in the port specific results.
3. Go to *SLA statistics*.
4. Select one of the filtering menus labelled as *Filter A1*, *Filter A2*, etc. (or *Filter B1*, *Filter B2*, etc in Port B).
   All the result menus related with the current filter are displayed.
5. Go to either *Availability statistics* or *Delay statistics*.
6. If you have chosen *Availability statistics* in the previous step then check the *Lost frames*, *FLR*, *SES*, *PEU (%)*, *Out-of-sequence frames* and *Duplicated frames* results.If you have chosen *Delay statistics* in the previous step then check the *Current, Maximum*, *Minimum Average, Standard dev.iation* and *Range* values of the *FTD* and the *Current, Average* and *Maximum* values of the *FDV*.

Table 6.11: SLA Delay Statistics

Field	Description
FTD (current)	Current value of the point-to-point Ethernet Frame Delay computed as specified in ITU-T Y.1563 and expressed in ms. To display the current FTD it is required a previous initialization of a test with *Run*.
FTD (maximum)	Peak value of FTD registered from the beginning of the test. The *FTD (max)* value is a packet by packet computed statistic. All relevant SLA packets are considered for calculation of this statistics.
FTD (minimum)	Minimum value of FTD registered from the beginning of the test. The *FTD (min)* value is a packet by packet computed statistic. All relevant SLA packets are considered for calculation of this statistics.
FTD (average)	Average of all registered FTD values from the beginning of the test. All relevant SLA packets are considered for calculation of this statistics (no sampling process is involved in the calculation of this statistic).
FTD (standard deviation)	Standard deviation (positive square root of the variance) corresponding with all the registered FTD values from the beginning of the test. The standard deviation quantifies the delay dispersion or delay variation found in the DUT / SUT.

Table 6.11: SLA Delay Statistics

Field	Description
FTD (range)	This performance metric is the result of subtracting *FTD (min)* from *FTD (max).* The range is an alternative way to the standard deviation to quantify the delay dispersion found in the DUT / SUT.
FDV (current)	Current value of the jitter computed as per RFC 3393 and RFC 1889. Delay variation is computed over consecutively transmitted packets. The jitter value is smoothed with the function defined in RFC 1889 before being displayed. The current FDV constitutes still another metric to quantify the delay variation in the DUT / SUT. To display the current jitter it is required a previous initialization of a test with *run*.
FDV (maximum)	Smoothed jitter maximum computed from the beginning of the test. The *FDV (max)* is a packet-by-packet statistic that does not involve any sampling process.
FDV (average)	Average of all individual delay variation values computed from the beginning of the test. Each individual delay variation is evaluated as the absolute value of the FTD associated to a given frame minus the FTD associated to the frame transmitted next. All possible consecutive frame transmission events are taken into account for the calculation of this performance metric. The only exception to this rule is if one or both frames are lost.

6.4.Traffic Capture

Tempo enables users to capture traffic at wirespeed by adding precise time stamps derived from a time reference (GNSS, ToD, IRIG-B) when available.

The capture engine stores traffic in fast RAM memory. This mechanism guarantees zero data loss even if the capture runs at 10 Gb/s but as the traffic is stored in volatile memory, every outcome has to be exported to USB or micro SD before starting a new capture. The captured traffic is also lost if the unit is restarted.

Current implementation of the traffic capture function enables capturing from Ethernet Port A only. Only the received traffic flows are captured. Traffic generated from port A will not be visible in the capture. It is necessary to remark that the previous explanation does not mean that Port B could not be used when the capture runs. The capture works in Ethernet endpoint, IP endpoint and even in IP through modes. Port B couldbe generating, analysing or forwarding traffic when the capture is running but no frame will be captured from this port.

6.4.1. Configuring the Capture

Capturing with Tempo is an extension of the multi-stream analysis performed by these units: Captured frames will be the outcome of matching the incoming traffic with the Port A filtering blocks. Every captured frame is labelled so that the matching filter can be identified. This is the same that in the per-flow bandwidth and SLA statistics that take the basis for traffic classification from the filters. A proper filter configuration is therefore important for capturing the right traffic. The detailed description of the capture configuration procedure is described below:

1. From the *Home* panel, go to *TEST*,
   The test configuration panel is displayed.
2. Go to *Protocol Analysis*
3. Go to *Capture*
4. Enable the traffic capture by setting the *Enable* control to *On*
5. Optionally, enable the *Wrap around mode* if you want the last captured frames to overwrite traffic captured previously when storage capacity is exhausted.
6. Configure *Filter* to add the filtering blocks you want the capture to take into account. In the current implementation, you can add up to eight filters from Port A.

Table 6.12: Capture Configuration

Metric	Description
Enable	It this setting is configured to On it enables the traffic capture function. Otherwise, the capture remains disabled.
Wrap around mode	Enables the wrap around mode for the capture function. This mode allows continuous frame capture beyond the capture buffer storage capacity at the price of losing information captured previously.
Capture direction	The current release supports capturing only in the receiving direction. For this reason this setting is statically configured to *RX*.
Filter	Allows the user to select the filters to be taken into account in the capture. At least one filter has to be configured to enable the frames to be captured. The filters selected here must be set to match the traffic to be captured.

7. Configure the filters you have added in the previous stream (See section 6.2).
8. Start the capture by pressing the *Run* button.

9. Use the *Filter statistics* (See section 6.3) and *Capture status* (See section 6.4.2) panel to display information about the ongoing capture
10. Stop the capture at any by pressing the *Run* button a second time.
    Note: Storage capacity is 128 MB in Port A. When this capacity runs out, capturing stops (or starts replacing previously captured traffic in the wrap around mode)
11. Download the capture from the Protocol Analysis panel (See section 6.4.3) using the web interface (See section 6.4.4).
    Note: Starting a new capture replaces the existing data by newly captured traffic. Restarting the unit deletes the last capture from the internal memory.

6.4.2. Controlling the Capture

You can always get real-time information about how many frames have been captured from the Filter statistics panel. The *Filter statistics* is useful to know which port and which filtering blocks are matching the traffic you receive from the network. Usage of the *Filter statistics* panel is explained in the section specifically devoted to filtering data (See section 6.3)

Table 6.13: Capture Status

Metric	Description
Status	Displays information about the current capture status. Itcan be any of the following: • *Idle*: The equipment is not capturing any frame. Typically this is because there is not any ongoing test or because there are no frames matching the required rules in the filter configuration or because there are no frames at all in the configured capture directions. • *Capturing*: The equipment is currently capturing frames. • *Memory full*: The storage capacity for captures if filled with data. The currently ongoing test does not stop when this condition is declared but the capture buffer is not able to capture more frames without deleting some of the stored data. If the wrap around mode is enabled, *Capturing* and *Memory full* are displayed at the same time when the capture buffer is full.
Packets stored	Provides information about the number of captured packets.
First capture at	Supplies the date and time corresponding to the first frame in the capture with the format *dd/MM/yyyy hh:mm:ss*.
Last capture at	Supplies the date and time corresponding to the first frame in the capture with the format *dd/MM/yyyy hh:mm:ss*.

Table 6.13: Capture Status

Metric	Description
Usage (%)	Displays amount of storage space filled with capture dataas a percentage of the total available storage bufferspace.

The second tool to be used to get information about captures is the *Capture status* panel. This panel displays miscellaneous details about the ongoing capture. Some results form this panel are relevant for drop actions as well. To display the Capture status panel follow this procedure:

1. From the *Home* panel, go to *Results*,
   The general results and statistics menu is displayed.
2. Enter in *Capture status*.
3. Check the *Dumping*, *Remaining capacity, Suppressed frames form port A* (drop actions only), *Suppressed frames from port B* (drop actions only) and *Suppressed frames* results.

6.4.3. Protocol Analysis

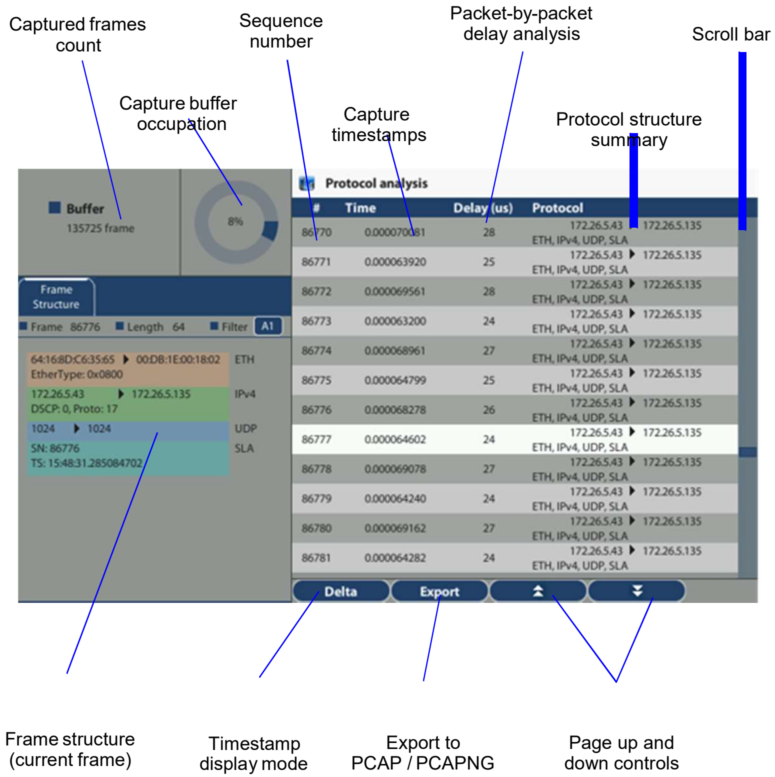
Tempo includes its own built in protocol analysis function which helps determining the frame structure and content from the captured data but it also provides valuable information related with timing including capture timestamps and packet-by- packet delay analysis performed over timestamped packets (PTP, NTP, GOOSE, SV, etc.).

The test unit is ready to run the protocol analysis once the packet capture process finishes. The procedure to display the *Protocol Analysis* panel is as follows:

1. From the *Home* panel, go to *Results*,
   The general results and statistics menu is displayed.
2. Enter in *Protocol analysis*.
3. Select a packet in the list with the help of the cursor, the scroll bar and the page up and down controls.
4. Check the sequence number (#), time stamp (*Time*), *Delay (us)* and protocol structure (*Protocol)*. If necessary, set the time stamp display mode with the corresponding contextual button. Check also the frame structure with the protocol layers different fields and the value assigned to the most important ofthem.
   Note: The tester includes packet dissection resources for several protocols including *DNS*, *ARP*, *DHCP*, *PTP*, *NTP*, *GOOSE* and *SV*.

The current capture is overwritten with new data if a new capture starts. Captures are also deleted when the unit is restarted if users do not export them to a USB memory or a micro SD card. There are two different ways to export captures. One of them is based on the Tempo web interface (See section 6.4.4). The other method, which starts once a USB memory stick or compatible micro SD card is attached to the unit, is described in the following lines:

1. From the *Home* panel, go to *Results*,
   The general results and statistics menu is displayed.
2. Enter in *Protocol analysis*.
3. Press the *Export* button.
4. Select the capture file format (**.pcap*, **.pcapng*), the *Filter* (from *A1* to *A8*) and the capture file name.
5. Press *Export*.
   Wait to the capture file to be exported.


Captured frames count
Sequence number
Packet-by-packet delay analysis
Scroll bar
Capture buffer occupation
Capture timestamps
Protocol structure summary
Frame structure (current frame)
Timestamp display mode
Export to PCAP / PCAPNG
Page up and down controls
Delta
Export
Frame Structure

Buffer
135725 frame

8%

Frame 86776 Length 64 Filter A1

64:16:8D:C6:35:65 ▶ 00:DB:1E:00:18:02 ETH
EtherType: 0x0800
172.26.5.43 ▶ 172.26.5.135 IPv4
DSCP: 0, Proto: 17
1024 ▶ 1024 UDP
SN: 86776 SLA
TS: 15:48:31.285084702

Protocol analysis

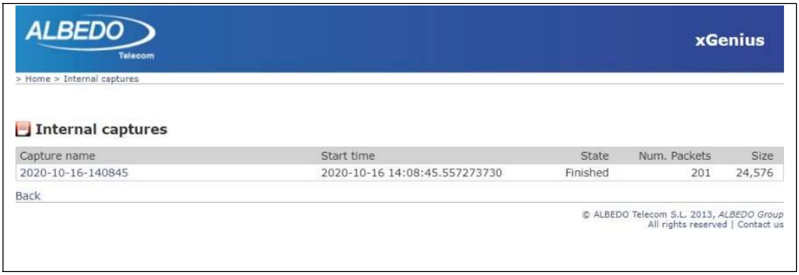
#	Time	Delay (us)	Protocol
86770	0.000070081	28	172.26.5.43 ▶ 172.26.5.135 ETH, IPv4, UDP, SLA
86771	0.000063920	25	172.26.5.43 ▶ 172.26.5.135 ETH, IPv4, UDP, SLA
86772	0.000069561	28	172.26.5.43 ▶ 172.26.5.135 ETH, IPv4, UDP, SLA
86773	0.000063200	24	172.26.5.43 ▶ 172.26.5.135 ETH, IPv4, UDP, SLA
86774	0.000068961	27	172.26.5.43 ▶ 172.26.5.135 ETH, IPv4, UDP, SLA
86775	0.000064799	25	172.26.5.43 ▶ 172.26.5.135 ETH, IPv4, UDP, SLA
86776	0.000068278	26	172.26.5.43 ▶ 172.26.5.135 ETH, IPv4, UDP, SLA
86777	0.000064602	24	172.26.5.43 ▶ 172.26.5.135 ETH, IPv4, UDP, SLA
86778	0.000069078	27	172.26.5.43 ▶ 172.26.5.135 ETH, IPv4, UDP, SLA
86779	0.000064240	24	172.26.5.43 ▶ 172.26.5.135 ETH, IPv4, UDP, SLA
86780	0.000069162	27	172.26.5.43 ▶ 172.26.5.135 ETH, IPv4, UDP, SLA
86781	0.000064282	24	172.26.5.43 ▶ 172.26.5.135 ETH, IPv4, UDP, SLA

Figure 6.2: Protocol analysis screen

6.4.4. Capture Management through the Web Interface

The alternative to the protocol analysis panel to export captures from Tempo is the web interface. To use the web interface you need to connect the management network connector to an Ethernet network and configure the management Ethernet interface (See section 6.3.1). Once you have done this, follow this procedure:

1. Open a browser in a computer with network connection.
2. Type the IP address you have assigned to the tester in the browser destination URL.
   The web interface home panel is displayed in the Internet browser.



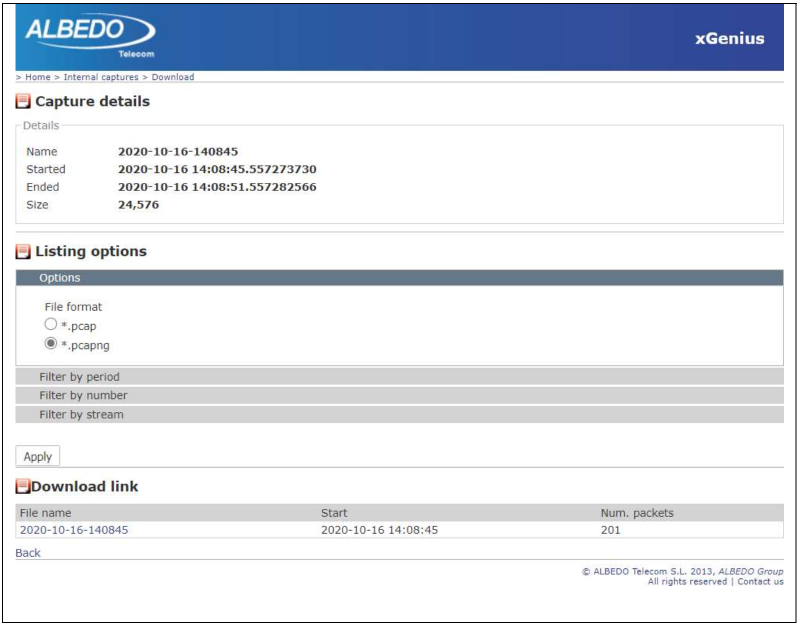
Internal captures

Capture name	Start time	State	Num. Packets	Size
2020-10-16-140845	2020-10-16 14:08:45.557273730	Finished	201	24,576

Back

© ALBEDO Telecom S.L. 2013, *ALBEDO Group*
All rights reserved | Contact us

(a)



Capture details

Details

Name	2020-10-16-140845
Started	2020-10-16 14:08:45.557273730
Ended	2020-10-16 14:08:51.557282566
Size	24,576

Listing options

Options

File format
○ *.pcap
● *.pcapng

Download link

File name	Start	Num. packets
2020-10-16-140845	2020-10-16 14:08:45	201

Back

© ALBEDO Telecom S.L. 2013, *ALBEDO Group*
All rights reserved | Contact us

(b)

Figure 6.3: Tempo web interface: (a) Capture list (b) Capture download panel with export filter selection.

3. Select the *Internal memory* link in the *Capture files* menu.
   A list with all the captures currently available for download is displayed.
   Note: The list is not available if there packet capture is not enabled in the unit (See section 6.4.1).
   Note: In Tempo the captures list could have one item at most because the older item is deleted every time a new capture is started.
4. Choose the capture that contains the traffic you want to export.
   The Capture download panel is displayed
5. Select the capture file format (**.pcap* or **.pcapng*) with the help of the *Options* menu and, if necessary, press *Apply* to confirm your selection.
6. Optionally, configure one or several export filters (See section 6.4.5).
7. Download the capture file by clicking at the hyper link displayed in the Download link table.
8. Open the capture file using WireShark or any other protocol analysis software compatible with the file format.

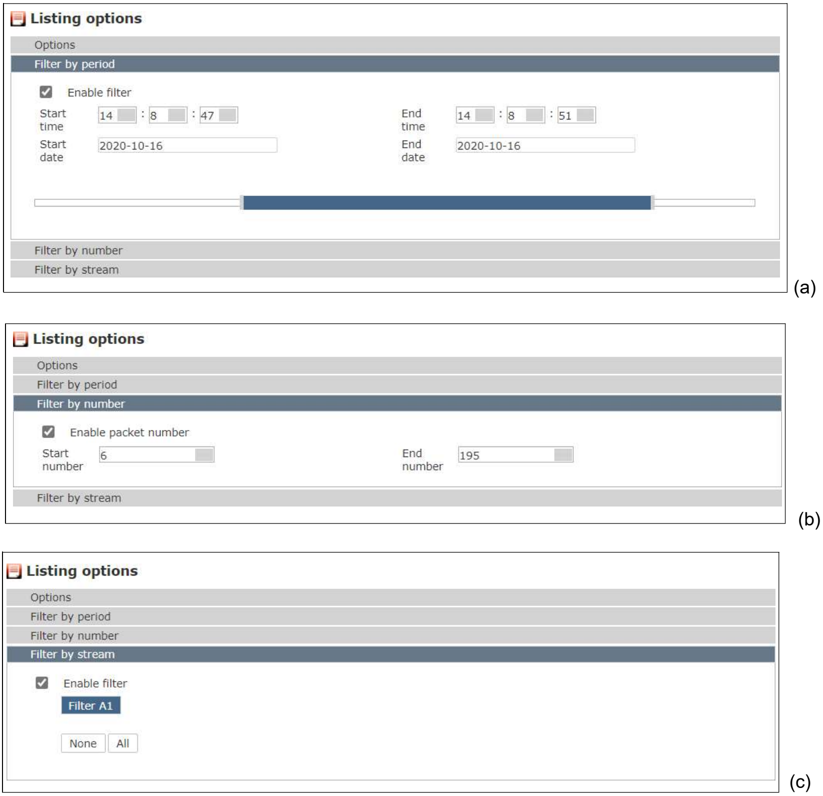
6.4.5. Using Export Filters

Tempo enables users to select the traffic to be exported from an existing capture once this capture has finished. The procedure to select the traffic to be exported is done just before the PCAP or PCAPNG file is generated and downloaded from the web browser.

To use export filters, proceed as explained in previous sections but enable and configure at least one export filter just before exporting to PCAP or PCAPNG formats. The detailed procedure is as follows

1. From the capture download panel in the web interface, configure the range of data to be exported by enabling (*Enable filter* check box) *Filter by period* and selecting the start and end date / time of the data to be exported.
2. Configure the number of packets to be exported by enabling (*Enable filter* check box) *Filter by number* configuring the initial and final packet index.
3. Configure the origin of data to be exported by enabling (*Enable filter* check box) *Filter by stream* and selecting the traffic flows to be exported.
   Note: When the frames are captured they are marked with flow identifier that depends on the filter matching each frame. These marks can be used to choose which frames to export once the capture has finished.

4. Press Apply and wait until the capture file is regenerated.



Listing options

Options

Filter by period

☑ Enable filter

Start time 14 : 8 : 47 End time 14 : 8 : 51

Start date 2020-10-16 End date 2020-10-16

Filter by number

Filter by stream

(a)

Listing options

Options

Filter by period

Filter by number

☑ Enable packet number

Start number 6 End number 195

Filter by stream

(b)

Listing options

Options

Filter by period

Filter by number

Filter by stream

☑ Enable filter

Filter A1

(c)

Figure 6.4: Tempo web interface: (a) *Filter by period* panel (b) *Filter by number* panel (c) *Filter by stream* panel.

Chapter 7
Automatic Performance Tests

Automatic tests are different to the measurements explained in previous chapters in that they are usually easier to configure and run. Specifically, the user does not need to worry about which bandwidth profile to use or which test payload to configure. However, users are still required to enter the correct MAC and IP addresses, CoS marks, and other frame and network configuration through the menu system (See section 4.1.2 and See section 4.2.4). Due to the way automatic tests use the bandwidth profile settings, the equipment may need to generate large amounts of traffic. This traffic may cause congestion in some unprepared networks and damage performance of any service already deployed. For this reason, users are advised to use automatic measurements with care.

The second relevant property of automatic tests is that they provide a clear pass or fail result that is easier to understand than a numeric latency figure or a bandwidth statistic. Thresholds for the pass / fail results can be tuned through specific menus.

Calnex Tempo currently supports three different automatic measurements: The IETF RFC 2544 test, the Ethernet service activation test methodology (eSAM) based on the ITU-T Y.1564 standard and the IETF RFC 6349 TCP throughput test. The first of them has been used for many years and its a very well established network benchmarking mechanism. The second has been introduced more recently but it has several advantages over the RFC 2544 tests like faster execution, support for multi-service environments and support for colored traffic. Finally, the RFC 6349 is specifically designed to TCP applications. TCP is connection oriented and it has its own frame structure, handshaking, flow control and congestion management mechanisms and for this reason testing TCP throughput is quite different to verification of non-connection oriented protocols such as UDP.

In all automatic tests described in this chapter, *Port A* and *Port B* have always different roles. *Port A* is always used for traffic generation and *Port B* is used only as an auxiliary port. In two-way or asymmetric tests *Port B* has no role at all and the traffic runs between *Port A* in the local unit and *Port A* in a unit installed in the remote end.bb

7.1.Performance Assessment with the RFC 2544 Test

The RFC 2544 is an IETF standard that describes benchmarking tests for network devices. Vendors can use these tests to measure and outline the performance characteristics of their Ethernet and IP switching equipment. As these tests follow standard procedures, they also make it easier for customers to make sense of the glitzy marketing-speak employed by most vendors.

The tests described in the document aim to evaluate how a device would act in a real situation. The RFC 2544 describes out-of-service tests, which means that real traffic must be stopped and the tester will generate specific frames to evaluate throughput, latency, frame loss rate, burst tolerance, overload conditions and recovery.

To configure an RFC 2544 follow these steps:

1. Make sure that your tester is connected to the network. The physical layer must be up and working (See section 4.1.1).
2. From the *Home* panel, go to *CONFIG*,
   The port setup panel is displayed.
3. Choose between *Ethernet endpoint* or *IP endpoint* with the *Mode* setting.
4. From the *Home* panel, go to *TEST*,
   The test configuration panel is displayed.
5. Go to *Performance test* and configure *RFC 2544*.
6. Go to *RFC 2544 configuration*.
   The panel with specific configuration of the RFC 2544 throughput, latency, frame loss, back-to-back frames and system recovery time tests is displayed.
7. Configure the test frame sizes with the help of the *Frame sizes* multiple selection list. The available frame sizes are: *64*, *128*, *256*, *512*, *1024*, *1280*, *1518* and *User-defined*.
8. If *User-defined* is enabled in the previous step, configure the user frame size to something between 64 and 10000 bytes through the *User frame size* control.
9. Configure the *Throughput test* (See section 7.1.1), *Latency test* (See section 7.1.2), *Frame Loss test* (See section 7.1.3), *Back-to-back test* (See section 7.1.4) and *System recovery test* (See section 7.1.5).
10. Leave *RFC 2544 configuration* and enter in *RFC 2544 objectives*.
11. Set the pass / fail thresholds for the throughput, latency, frame loss, back-to-back frames and system recovery tests from the *Performance objectives* menu (See section 7.1.6).
12. Leave the *RFC 2544 objectives* and *Performance test* panels.
13. Go to *Test mode*
14. Depending on your test setup (See section 2.2.3), configure *Test method* to *One-way (A > B)*, *Two-way (A > A)*, *Upstream* or *Downstream*.
15. If you have configured either the *Upstream* or *Downstream* test modes, configure *Remote unit MAC* (in *Ethernet endpoint* mode) or *Remote unit IP* (in I*P endpoint*

mode).
Note: A unit configured in *Remotely managed* mode has to be installed and configured in the remote end before any asymmetric test can be run (See section 7.4).

16. From the *Home* panel, go to *CONFIG*,
    The port setup panel is displayed.
17. Configure the *Frame layer* (See section 4.1.2) in *Port A* for *Flow A1*. Parameters to be configured are source and destination MAC addresses, VLANs, etc.
    Note: All flows different to *Flow A1* are disabled in RFC 2544 tests. This test is only compatible with a single flow transmission.
    Note: If you are running an *Upstream* asymmetric test in *Ethernet endpoint* mode, you are allowed to configure the *Destination MAC address from* field to *Remote*. In this way, you are setting the destination MAC address to be the responder address.
    Note: If you are running a *Downstream* asymmetric test, you need to think in the port settings you configure as the configuration for the responder device (who is going to be the traffic generator). For this reason you are allowed to configure the *Source MAC address from* field to *Remote*. This setting configures the source address in the traffic generator (the responder device, in this mode) to be the own responder address.
18. If you are working in *IP endpoint* mode, configure the *Local profile* (See section 2.3) and the *Network layer* (See section 4.2.4). Parameters to be configured are IP addresses, DSCPs, etc.
    Note: If you are running an *Upstream* asymmetric test in *IP endpoint* mode, you are allowed to configure the *Destination IP address from* field to *Remote*. In this way, you are setting the destination IP address to be the responder address.
    Note: In the same way than in *Downstream* Ethernet endpoint tests, you need to think in the port settings you configure as the configuration for the responder device. For this reason you are allowed to configure the *Source IP address from* field to *Remote*. This setting configures the source address in the traffic generator to be the own responder IP address.

You can optionally attach a GNSS receiver to the test units (controller and responder) to measure one way delay in the RFC 2544 test (See section 2.6.2). To do that, follow these steps:

1. From the *Home* panel, go to *CONFIG*,
   The port setup panel is displayed.
2. Go to *Reference clock*.
3. Configure Input clock to GNSS

7.1.1. Throughput

The aim of a *throughput test* is to determine the maximum number of frames per second that the device can process and forward without dropping or losing any. Put in simple terms, the procedure used to compute the throughput is as follows:

1. Send a certain number of frames at a specific rate through the DUT / SUT and count the frames transmitted by the DUT / SUT.
2. If the count of transmitted frames is equal to the count of received frames, increase the transmission rate and re-run the test. Otherwise, reduce the transmission rate to be used in the next trial.
3. Re-run the test until fewer frames are transmitted than received by the DUT / SUT. The throughput is the fastest rate at which the count of test frames transmitted by the DUT is equal to the number of test frames sent to it by the measurement equipment.

Table 7.1: RFC 2544 Throughput Test Settings

Setting	Description
Enable	Enables or disables the RFC 2544 throughput test. The throughput test will not run with the remaining RFC 2544 tests if they are not previously enabled. The *Latency* and *System recovery* tests depend on the throughput results and they are disabled if the throughput test is also disabled.
Maximum rate (%)	It is the maximum bit rate the DUT / SUT supports due policing or other bandwidth limiting mechanisms. The *Maximum rate (%)* constitutes the upper level of the throughput result. The *Maximum rate (%)* is configured as a percentage of the nominal transmission rate configured through link auto-negotiation or fixed by the network administrators. If the DUT / SUT is not using bandwidth limiting mechanisms or the maximum rate is unknown, configure this field to 100 %. Test results should not change but it will take more time to get the same results with the same accuracy level.
Resolution (%)	Minimum throughput, expressed as a percentage of the nominal channel capacity, that can be distinguished by the RFC 2544 throughput algorithm. This algorithm finishes when the distance between the real throughput and the value estimated by the algorithm is smaller than the resolution. Configuring an smaller value of the resolution increases measurement accuracy but also increases the time needed to finish the throughput test.

Table 7.1: RFC 2544 Throughput Test Settings

Setting	Description
Trial duration (s.)	This value corresponds with the duration of asingle throughput trial test expressed in seconds. Each algorithm test cycle contains one trial. The equipment transmits test traffic during the time specified by this setting before deciding by means the analysis of the number of lost frames whether to continue or not. Some equipments may need some time before they start dropping frames. If the trial duration is too short this may cause the estimated throughput to be larger than it will in stationary transmission conditions.
Max. frame loss (%)	The equipment decides whether it is operating above or below the actual DUT / SUT throughput by comparing the number of transmitted and received frames. It decides that the current transmission rate is higher than the real throughput if the frame loss ratio is larger than the *Max.frame loss* (%) configured here. In the same way, the tester decides that the current test rate is smaller than the actual throughput if the computed frame loss ratio is smaller than the *Max. frame loss (%)*.

7.1.2. Latency

This test determines the latency inherent in the DUT / SUT. The initial data rate is based on the results of the throughput test. Typically, packets are timestamped using the SLA payload (See section 4.1.4, See section 4.2.6), and the time they take to travel through the DUT / SUT is measured.

In order to determine the latency you usually first measure the throughput for the DUT / SUT at each of the defined frame sizes, and send a stream of frames through the DUT / SUT at the determined throughput rate to a specific destination. If you don’t measure throughput the latency will be measured at the nominal capacity for the transmission medium.

The time at which this frame is completely transmitted is recorded, and this will be timestamp A. The receiver of the test equipment must recognize the tag information in the frame stream and record the reception time of the tagged frame. This will be timestamp B. The latency is the difference between timestamp B and timestamp A, according to the definition found in RFC 1242.

Table 7.2: RFC 2544 Latency Test Settings

Setting	Description
Enable	Enables or disables the RFC 2544 latency test. The latency test will not be executed if is not previously enabled by this control.
Trial duration (s.)	This value corresponds with the duration of a single latency trial test expressed in seconds. For each frame size, the RFC 2544 algorithm measures the latency several times. This parameter configures the duration of each latency measurement.
Rate (% throughput result)	Enables the user to configure which percentage of the throughput rate is used to measure the latency in the testing path. By default, the testing rate is set to the transmission channel throughput but results may be different if the test runs at a lower rate.
Iterations	This parameter corresponds with the number of times the latency is measured for every frame size.
Statistics	Sets which delay statistic is used to compute this test results. The default is to offer results based on the average delay but users may decide to use maximum or minimum delays instead.

7.1.3. Frame Loss

The aim of this test is to determine the frame loss ratio through the entire range of input data rates and frame sizes. The procedure is the following:

1. Send a certain number of frames at a specific rate through the DUT / SUT, counting the frames transmitted and received and computing the frame loss ratio. The first trial should be run for the frame rate that is 100% of the maximum rate supported by the interface.
2. Repeat the procedure for the speed that corresponds to the next test bitrate.

3. Continue this sequence (reducing the bit rate in every step) until there are two consecutive trials where no frames are lost.

Table 7.3: RFC 2544 Frame Loss Test Settings

Setting	Description
Enable	Enables or disables the RFC 2544 frame loss test. The frame loss test will not be executed if is not previously enabled by this control.
Resolution (%)	Measures the decrease in terms of bit rate the tester uses to measure frame loss expressed as a percentage of the nominal transmission capacity. For example if throughput result is 100% for one specific frame size and this field is set to 10%, then frame loss will be evaluated for 100%, 90%, 80%... of the transmission medium capacity. If frame loss is configured to 1%, the bit rates used in consecutive trials will be 100%, 99%, 98%... Setting an smaller *Resolution (%)* increases frame loss test accuracy but the tame it takes to finish the test is also increased.
Trial duration (s.)	This value corresponds with the duration of a single frame loss trial test expressed in seconds. For each configured frame size and load, the equipment sends and analyses traffic for a time period specified by this field. Longer trial duration periods tend to give more accurate frame loss results but they make measurements longer.

7.1.4. Back-to-Back Frames

A back-to-back frames test determines the *node buffer capacity* by sending bursts of traffic at the highest theoretical rate, and then measuring the longest burst where no packets are dropped. The test procedure is as follows:

1. Send a burst of frames with minimum inter-frame gaps to the DUT / SUT, and count the number of frames forwarded.
2. If the count of transmitted frames is equal to the number of frames forwarded, increase the length of the burst and re-run the test. If the number of forwarded frames is less than the number transmitted, reduce the length of the burst and re-run the test.
3. Continue until the back-to-back frames results has been computed with acceptable accuracy.

The back-to-back value is the number of frames in the longest burst that the DUT / SUT can handle without losing any frame. It is recommended to run the test for atleast

2 seconds, and it should be repeated at least 50 times with the average of the recorded values being reported.

Table 7.4: RFC 2544 Back-to-back Test Settings

Setting	Description
Enable	Enables or disables the RFC 2544 back-to-back frames test. The back-to-back frames test will not be executed if is not previously enabled by this control.
Maximum burst length (fr.)	This is the maximum frame burst to be used in an back-to-back frames test trial. The DUT / SUT should drop some frames when it receives a burst with the length configured in this field. If the actual back-to-back frames result is larger than the *Maximum burst length (fr.)*, the equipment will be unable to find it.
Resolution (fr.)	It is the minimum back-to-back frames result the equipment distinguishes as different results. When a test cycle finishes, the measurement algorithm compares the burst length with the result of the previous cycle. If the difference between them is smaller than the resolution, then the algorithm terminates. The final back-to-back result is the one computed in the last cycle.
Iterations	Configures the number of bursts sent per test cycle. Increasing *Iterations* makes the back-to-back test result more reliable but it also increases the overall testing time.

7.1.5. System Recovery

This test determines the node speed at which the DUT / SUT recovers from an overload condition. The procedure is as follows:

1. Measure the throughput for the DUT / SUT at each of the listed frame sizes.
2. Send a stream of frames at a rate that is 110% of the recorded throughput rate or the maximum rate for the media, whichever is lower, for at least 60 seconds.
3. At Timestamp A, reduce the frame rate to 50% of the above rate and record the time of the last frame lost (Timestamp B). The system recovery time is calculated by subtracting Timestamp B from Timestamp A. The test must be repeated a number of times, and the average of the recorded values is reported.

The system recovery results should be reported as a table, with a row for each of the tested frame sizes. There should be columns for the frame size, the frame rate used as the throughput rate for each type of data stream tested, and for the measured recovery time for each type of data stream tested.

Table 7.5: RFC 2544 System Recovery Test Settings

Setting	Description
Enable	Enables or disables the RFC 2544 system recovery test. The system recovery test will not be executed if is not previously enabled by this control.
Trial duration (s.)	Time, computed in seconds, the DUT / SUT is overloaded by frame transmission above the recorded throughput value.
Iterations	Number of times the recovery time is measured in onetest cycle. The final value of the recovery time will be the averaged value computed for each iterations. The more iterations per test cycle the more reliable the test results are. However, increasing the iterations increases the total testing time as well.

7.1.6. Configuration Pass / Fail Thresholds

One of the advantages of the RFC 2544 tests is the ability to supply a clear pass / fail results based on certain thresholds configured before the test start. To configure the pass / fail thresholds follow these steps:

Table 7.6: RFC 2544 Performance Objectives

Setting	Description
Throughput	Sets a performance objective for the RFC 2544 throughput test. The test will be considered to fail if the measured throughput is smaller that the threshold and it will be passed otherwise.
Latency	Sets a performance objective for the RFC 2544 latency test. The test is considered to fail if the result is larger than the threshold and it is considered to pass otherwise.
Frame loss	Configures an performance objective for the RFC 2544 frame loss test. The test is considered to fail if there is at least one result within the frame length and bit rate ranges which produces a frame loss figure larger than the threshold. The test is considered to pass otherwise.

Table 7.6: RFC 2544 Performance Objectives

Setting	Description
Back-to-back frames	Sets a performance objective for the RFC 2544 back-to-back frames test. The test is considered to fail if the back-to-back frames result is smaller than the configured threshold and it is considered to pass otherwise.
System recovery	Sets the performance objective for the RFC 2544 system recovery time test. The test fails if the system recovery time result is longer than the threshold and passes otherwise.

1. From the *Home* panel, go to *TEST*,
   The test configuration panel is displayed.
2. Go to *Performance objectives*,
3. Select *RFC 2544*.
   Note: You must enable the RFC 2544 test before you are allowed to enter in this menu.
4. Enter the thresholds for *Minimun throughput (%)*, *Maximum latency*, *Maximum frame loss (%)*, *Minimum frame burst (fr)*, *Maximum recovery time*.
   Note: Each specific test has to be individually enabled before you can set the performance objective for it.

7.1.7. Getting Test Results

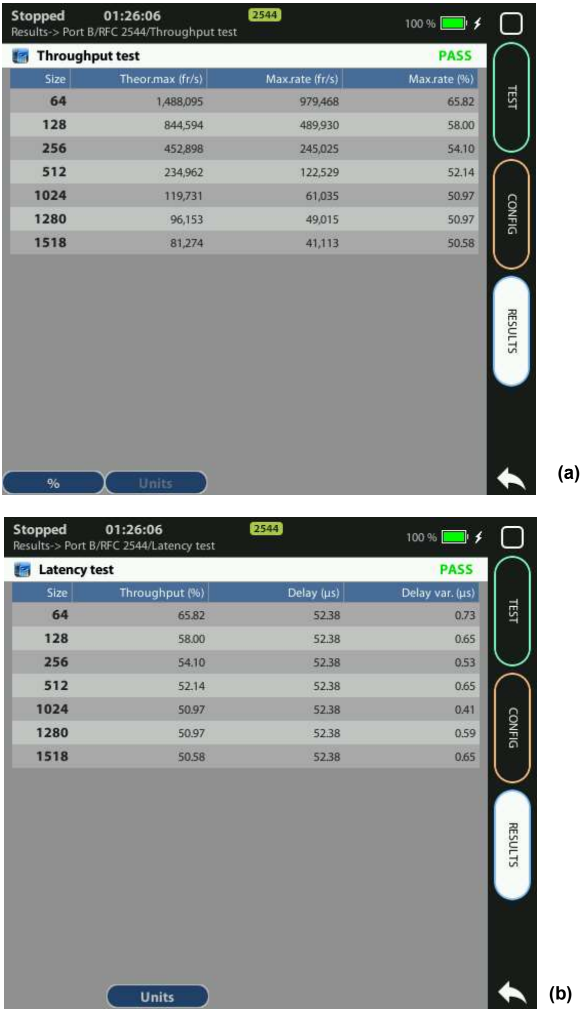
The RFC 2544 provides a description of the way test results must be presented to the user. Normally, these results are displayed as tables. Each row represents the test frame length or bit rate and columns are usually test results like throughput, latency or others.

The RFC 2544 results can be evaluated as pass or fail. Failed results are represented with red color. One test is considered to fail it at least one test result fails. The whole RFC 2544 fails if one particular test result fails. The global Pass / Fail can be checked at any moment, even before the end of the test from the *Summary* panel.

Once the test has been configured, it can be started at any time with the help of the *run* button. You can wait to the test to finish but it is also possible to check partial test results at any moment. To do that follow these steps:

1. From the *Home* panel, go to *RESULTS*,
   The test port results panel is displayed.
2. Select either *Port A or Port B* to enter in the port specific results.
   Note: If you have configured *Test method* to *One-way (A > B),* the RFC 2544

results are available in *Port B*. On the other hand, if you have configured *Two-way (A > A)*, Upstream or *Downstream*, the RFC 2544 results are available in *Port A*.



Stopped 01:26:06 2544 100 %

Results-> Port B/RFC 2544/Throughput test

Throughput test PASS

Size	Theor.max (fr/s)	Max.rate (fr/s)	Max.rate (%)
64	1,488,095	979,468	65.82
128	844,594	489,930	58.00
256	452,898	245,025	54.10
512	234,962	122,529	52.14
1024	119,731	61,035	50.97
1280	96,153	49,015	50.97
1518	81,274	41,113	50.58

Stopped 01:26:06 2544 100 %

Results-> Port B/RFC 2544/Latency test

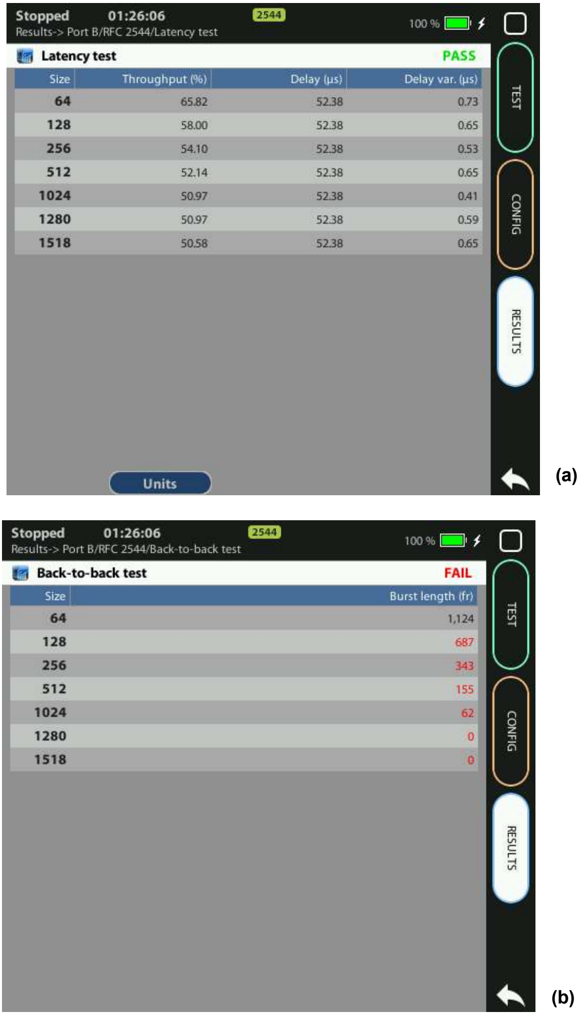
Latency test PASS

Size	Throughput (%)	Delay (µs)	Delay var. (µs)
64	65.82	52.38	0.73
128	58.00	52.38	0.65
256	54.10	52.38	0.53
512	52.14	52.38	0.65
1024	50.97	52.38	0.41
1280	50.97	52.38	0.59
1518	50.58	52.38	0.65

Figure 7.1: RFC 2544 test results: (a) Throughput results table, (b) Latency results table.

3. Select *RFC 2544*.
4. Check the *Status* field to know the pass / fail test result. If the test has not yet finished, this field will display a *In progress* message. If the equipment detects an error during text execution it will display an error message.

5. Check the *Current stage* and *In progress* fields to know what is doing the tester in the current moment and which is the current test progress.



Stopped 01:26:06 2544 100 %

Results-> Port B/RFC 2544/Latency test

Latency test PASS

Size	Throughput (%)	Delay (µs)	Delay var. (µs)
64	65.82	52.38	0.73
128	58.00	52.38	0.65
256	54.10	52.38	0.53
512	52.14	52.38	0.65
1024	50.97	52.38	0.41
1280	50.97	52.38	0.59
1518	50.58	52.38	0.65

Stopped 01:26:06 2544 100 %

Results-> Port B/RFC 2544/Back-to-back test

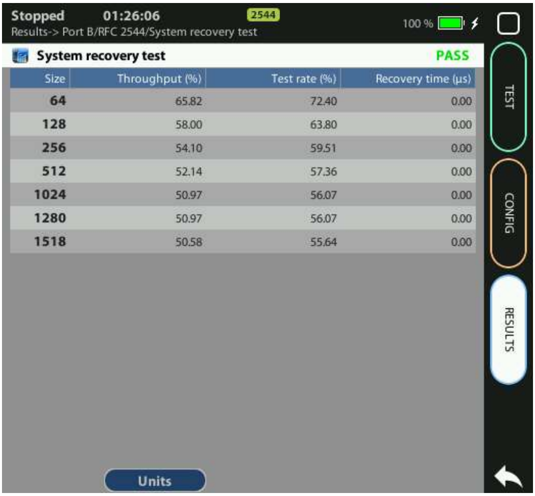
Back-to-back test FAIL

Size	Burst length (fr)
64	1,124
128	687
256	343
512	155
1024	62
1280	0
1518	0

Figure 7.2: RFC 2544 test results: (a) Frame loss result table, (b) Back-to-back frames result table.

6. Go to the *Throughput test*, *Latency test*, *Frame lost test*, *Back-to-back test* and *System recovery test* and check the detail led results for each of them.
   Note: Test results depend on the frame length and some of them also on the throughput. For this reason, RFC 2544 result tables depend on both magnitudes:

Size and *Throughput (%)*. *Throughput (%)* represents the bit rate used for testing latency and frame loss. It can be the previously measured maximum rate attainable bit rate expressed as a percentage of the nominal interface rate (10 Mb/s, 100 Mb/s, 1000 Mb/s, 10 Gb/s) or a different value depending on the particular test settings.



Stopped 01:26:06 2544
Results-> Port B/RFC 2544/System recovery test

System recovery test PASS

Size	Throughput (%)	Test rate (%)	Recovery time (µs)
64	65.82	72.40	0.00
128	58.00	63.80	0.00
256	54.10	59.51	0.00
512	52.14	57.36	0.00
1024	50.97	56.07	0.00
1280	50.97	56.07	0.00
1518	50.58	55.64	0.00

Figure 7.3: RFC 2544 System recovery time results table.

Note: The system recovery time tests sends traffic above the throughput value in order to overload the DUT / SUT, the test traffic in this case is indicated in the results table by means the *Test rate (%)* column.

Table 7.7: RFC 2544 Test Results

Setting	Description
Theoret. max rate (fr/s)	Theoretical maximum rate attainable in the transmission medium expressed in frames per second. In an Ethernet link, this rate is calculated as nominal transmission capacity in bits per second (10 Mb/s, 100 Mb/s, 1000 Mb/s, 10 Gb/s) divided by the frame bits (including the 64-bit preamble and the 96-bit interframe gap). The theoretical maximum rate result is available in the *Throughput test* result table.

Table 7.7: RFC 2544 Test Results

Setting	Description
Measured max rate (fr/s)	Measured maximum rate attainable in the transmission medium expressed in frames per second. This result is always smaller or equal than the theoretical maximum rate result. The measured maximum rate result is available in the *Throughput test* result table
Delay (μs)	Latency result measured in microseconds. The delay result has to be understood as the one-way delay if the test is configured as a *One-way (A > B), Upstream* or *Downstream* test or as the round-trip delay if the test is configured as *Two-way (A > A)*. In many setups the round-trip delay is roughly twice that the one-way delay but in asymmetric setups this is not true anymore.
Delay var (μs)	Delay variation measured in microseconds. The delay variation is computed as specified in IETF RFC 3393 and it is to be understood as a one-way delay metric if the test is configured as a *One-way (A > B), Upstream* or *Downstream* test or as a two-way metric if the test method is *Two-way (A > A)*. In asymmetric tests this metric is also one-way and corresponds to the upstream or downstream path depending on the configure test method.
Frame loss (%)	Frame loss result expressed as a percentage of the total amount of frames transmitted in the trial for an specific frame length and throughput.
Burst length (fr)	Longest burst accepted by the DUT / SUT which produces no packet loss.
Recovery time (μs)	Time invested to recover from an overload condition expressed in microseconds.

7.1.8. Generation of RFC 2544 Result Reports

An essential part of standardized network testing is report generation. Reports summarize test results in a document that can be edited or shared with the customer. RFC 2544 reports include a text header with basic information about the test like start time, duration and configuration. Test results are presented in tables. There is one table for each test: throughput, latency, frame loss, back-to-back frames and system recovery time. All results include a Pass / Fail indication. The report also includes a global Pass / Fail indication which summarizes all test results: It follows an example of a typical RFC 2544 report as is generated by the test unit:

```
RFC 2544 Test Report

Report name              2012-11-22-185949
Customer
Department
Company
Location
Operator
Start Time               Thu Nov 22 18:59:49 2012
Elapsed Time             11:16:44
Test Unit                Ether.Giga Gigabit Ethernet Tester
Serial number            MEM0009P
Software version         1.13.35


Global results

Status                             FAIL
Completed                          100%


Test Unit Configuration

Mode                               IP endpoint
Test method                        Two-way (A > A)

                                                 Port A              Port B
Port mode                                         TX/RX            Loopback
Connector                                    Electrical          Electrical
Encapsulation                                      None
Source MAC address                    00:DB:1E:00:01:10
Destination MAC address               00:DB:1E:00:01:11
Address range size                                 ----
C-VID                                              ----
C-VLAN priority                                    ----
S-VID                                              ----
S-VLAN priority                                    ----
DEI                                                ----

Source IPv4 address                         172.26.3.23
Destination IPv4 address                    172.26.4.24
Destination host name                              ----
Address range size                                 ----
DSCP                                                  0

Performance objectives

Minimum throughput (%)                           50.000
Maximum latency                               10.000 ms
Maximum frame loss (%)                            1.000
Minimum frame burst (fr)                           1000
Maximum recovery time                         10.000 ms


Throughput test

    Frame sizes  Theor.max (fr/s)   Max.rate (fr/s)      Max.rate (%)      Sta-
tus
            64          148,809          40,399           27.140        FAIL
           128           84,459          39,755           47.070        FAIL
           256           45,289          39,009           86.130        PASS
           512           23,496          23,496          100.000        PASS
```

```
          1024          11,973          11,973          100.000          PASS
          1280           9,615           9,615          100.000          PASS
          1518           8,127           8,127          100.000          PASS


Latency test

   Frame sizes      Throughput (%)        Delay      Delay var.        Status
            64              27.140    778.03 us        14.62 us          PASS
           128              47.070     84.47 us        14.23 us          PASS
           256              86.130    228.79 us         5.04 us          PASS
           512             100.000    172.88 us         3.65 us          PASS
          1024             100.000    140.27 us         4.99 us          PASS
          1280             100.000    162.50 us         3.80 us          PASS
          1518             100.000    185.06 us         3.56 us          PASS


Frame loss test

   Throughput (%)       64      128      256      512     1024     1280     1518
           100.00   73.126   52.885   13.869    0.000    0.000    0.000    0.000
            90.00   70.086   47.603    4.368    0.000    0.000    0.000    0.000
            80.00   66.364   40.995    0.000      ---      ---      ---      ---
            70.00   61.527   32.571    0.000      ---      ---      ---      ---
            60.00   55.078   21.274      ---      ---      ---      ---      ---
            50.00   46.084    5.506      ---      ---      ---      ---      ---
            40.00   32.623    0.000      ---      ---      ---      ---      ---
            30.00   10.208    0.000      ---      ---      ---      ---      ---
            20.00    0.000      ---      ---      ---      ---      ---      ---
            10.00    0.000      ---      ---      ---      ---      ---      ---
                      FAIL     FAIL     FAIL     PASS     PASS     PASS     PASS


Back-to-back test

   Frame sizes             Burst length (fr)                              Status
            64                        46,875                                PASS
           128                        46,875                                PASS
           256                        46,875                                PASS
           512                     3,000,000                                PASS
          1024                     3,000,000                                PASS
          1280                     3,000,000                                PASS
          1518                     3,000,000                                PASS


System recovery test

   Frame sizes     Throughput (%)      Recovery time                      Status
            64              27.14      620.400 us                           PASS
           128              47.07      906.000 us                           PASS
           256              86.13      335.000 us                           PASS
           512             100.00        0.000 us                           PASS
          1024             100.00        0.000 us                           PASS
          1280             100.00        0.000 us                           PASS
          1518             100.00        0.000 us                           PASS
```

7.2.Performance Assessment with the eSAM Test

Ethernet service activation though eSAM defined in ITU-T 1564 has arisen as an alternative to RFC 2544 verification. Unlike the RFC 2544, eSAM is designed for Ethernet service activation from the beginning. The advantages of eSAM in front of RFC 2544 are summarized in the following points:

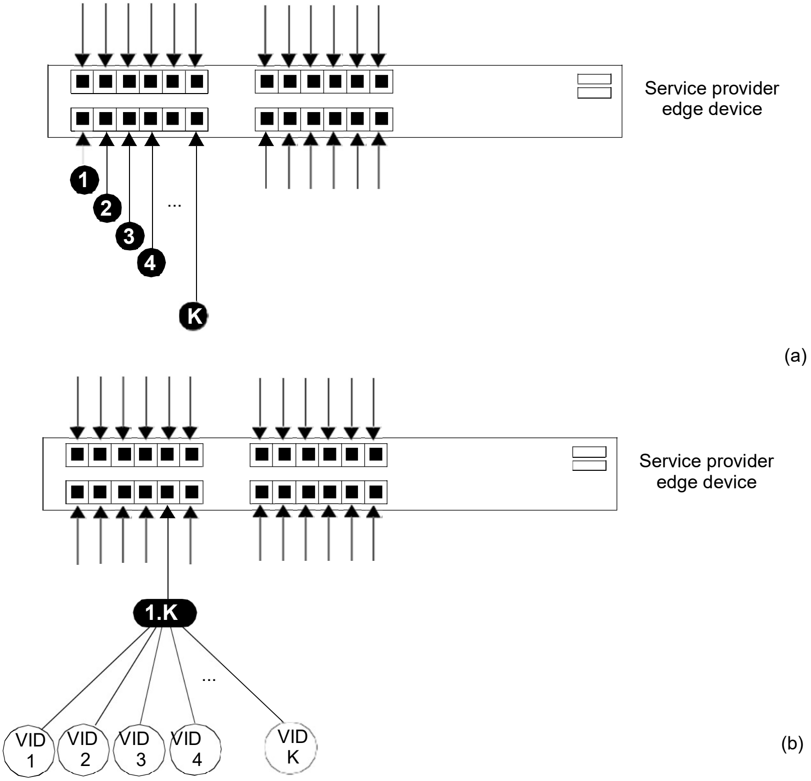


Figure 7.4: (a) Port based Ethernet service, one service per port. (b) Ethernet service multiplexing based on service delimiting markers like the VLAN tag.

1. *Faster execution*: An standard eSAM test is made up of a short configuration test and a longer performance test. If the configuration test fails there is no need to execute the long performance test. The result is that network administrators have time to correct any configuration issue before having to wait for the complete test execution.
2. *FDV results*. Frame Delay Variation (FDV) is a key metric to evaluate network performance. FDV is very sensitive to congestion and other degradations that affect

end-to-end network performance and it is therefore an essential parameter to measure.

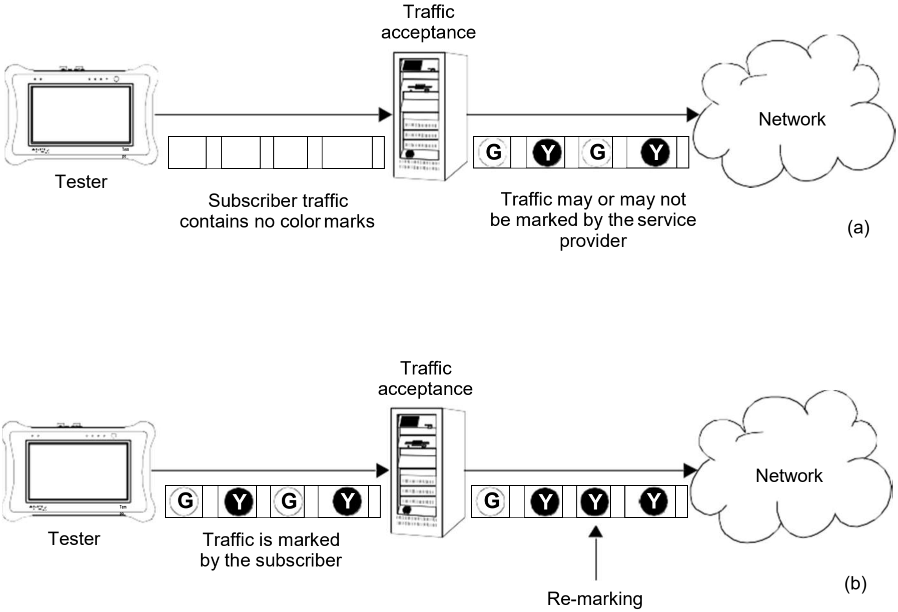

Traffic acceptance
Tester
Network
G
Y
G
Y
Subscriber traffic contains no color marks
Traffic may or may not be marked by the service provider
(a)
Traffic acceptance
Tester
Network
G
Y
G
Y
G
Y
Y
Y
Traffic is marked by the subscriber
Re-marking
(b)

Figure 7.5: (a) Non-color-aware service. It the service provider is wiling to implement different transmission priorities for this service, marking will have to be carried out by the access network by means some traffic classification algorithm. (b) In a color-aware service subscribers mark their own traffic from the beginning. The service provider may remark some traffic depending on the traffic acceptance algorithm.

3. *Compatible with multi-service environments*: Modern Ethernet services may be port based but service multiplexing in the same port by means some service delimiting tag is also very popular. The eSAM test has been designed to operate in environments using service multiplexing. In this case, all services are simultaneously tested and independent results are given for each of them.
4. *Supports color-aware traffic*: The eSAM test is compatible with color markers used by some service providers to enable the different performance levels in their applications. Color markers classify the network traffic in three sets: *green* traffic is transmitted within the delay and frame loss ratio limits guaranteed by the SLA agreement, *yellow* traffic is transmitted but the SLA agreement performance limits do not apply for it, and finally *red* traffic is discarded and not transmitted (red traffic is therefore never seen in the network). Common color markers used in practical

applications are the DSCP (Layer 3) and the VLAN priority bits (Layer 2). The latter requires the subscriber frames to be encapsulated in VLAN tagged frames.

7.2.1. Bandwidth Profiles for Ethernet Services

To see how eSAM works it is essential to understand how Ethernet services are defined. Network operators have at their disposal the tools that enable them to define their services with great flexibility. The information rate associated with Ethernet service is not limited to the nominal speed of the access network interface. For example, certain operator way want to define a 2 Mb/s service over an optical Gigabit Ethernet interface.

Performance in terms of delay, packet loss and other metrics is applied to traffic flows defined by their generation statistics or bandwidth profile. The mechanism used by service providers to make sure the ingress traffic has the correct bandwidth profile is admission control. Once the Ethernet access has been set up, the service provider performs admission control over the customer traffic at the user-network interface. Admission control for Ethernet services uses bandwidth profiles based on four parameters initially defined by the *Metro Ethernet Forum* (MEF):

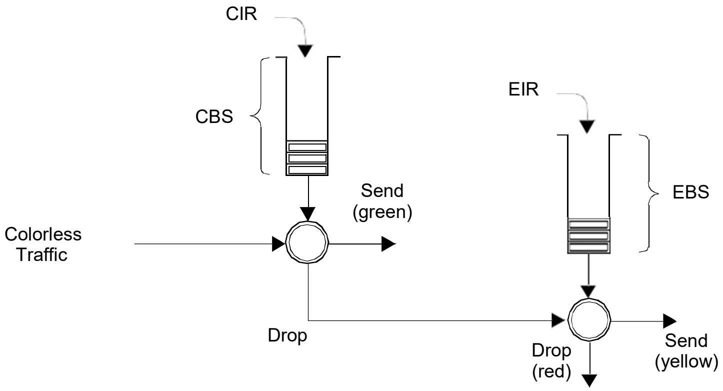


Figure 7.6: Two-rate Three color marker (trTCM). Policing algorithm.

- *Committed Information Rate (CIR)*: Rate up to which service frames are delivered as per the service performance objectives.
- *Committed Burst Size (CBS)*: Maximum number of bytes up to which service frames may be sent as per the service performance objectives without considering the CIR.
- *Excess Information Rate (EIR)*: Rate up to which service frames are still delivered but they are not subject to any performance objective.
- *Excess Burst Size (EBS)*: The number of bytes up to which service frames are sent (without performance objectives), even if they are out of the EIR threshold.

The MEF specifies the RFC 2698 *Two-rate Three-Color Marker* (trTCM) as the admission control mechanism for carrier Ethernet services. The trTCM is obtained by chaining two simple token bucket policers. Tokens fill the main bucket until they reach the capacity given by the CBS parameter, at a rate given by the CIR parameter. The secondary bucket is filled with tokens with the EIR rate until they reach the capacity given by the EBS parameter.

The traffic that passes through the first bucket (green traffic) is delivered with the QoS agreed with the service provider, but any traffic that passes through the secondary bucket (yellow traffic) is re-classified and delivered as best-effort traffic, or it is given a low priority. Non-conforming traffic (red traffic) is dropped.

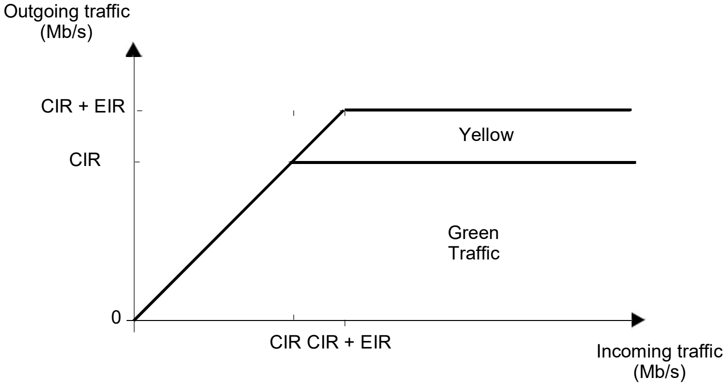
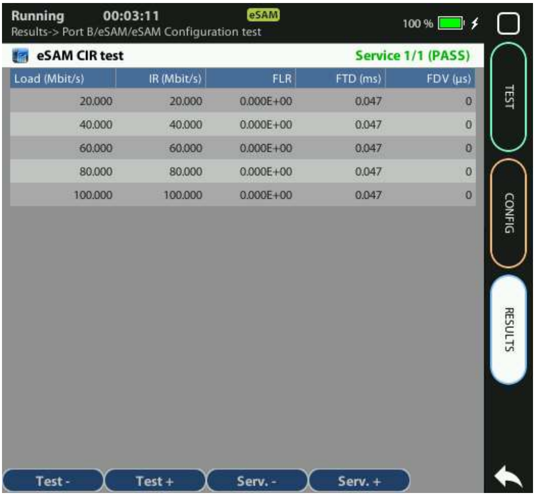


Figure 7.7: The amount of traffic that crosses an admission control filter. Graphics represent steady states, traffic is usually allowed to be greater than the CIR and EIR for short periods of time. Traffic delivery is guaranteed if the rate is smaller than the CIR. Excess traffic (EIR traffic) is delivered as well, but it is marked as low priority and usually discarded first if congestion occurs.

Note than the best effort classical service can be obtained simply by setting the CIR parameter to zero. Moreover, service providers may allow their subscribers to add their color marks to the traffic they generate before the traffic admission algorithm is applied. This kind of pre-marking transfers more control on the application performance to the end user. However, admission control is necessary even in this case and frame remarking is done on non-conforming traffic anyway.



Running 00:03:11

Results-> Port B/eSAM/eSAM Configuration test

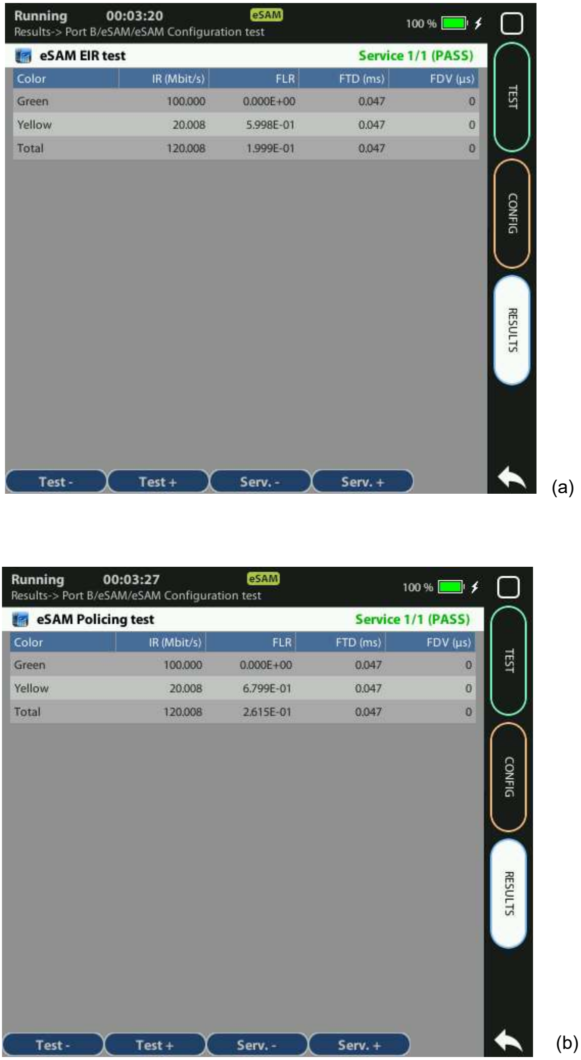
eSAM CIR test

Service 1/1 (PASS)

Load (Mbit/s)	IR (Mbit/s)	FLR	FTD (ms)	FDV (µs)
20.000	20.000	0.000E+00	0.047	0
40.000	40.000	0.000E+00	0.047	0
60.000	60.000	0.000E+00	0.047	0
80.000	80.000	0.000E+00	0.047	0
100.000	100.000	0.000E+00	0.047	0

Figure 7.8: CIR test results as presented by Tempo.

The basic purpose of eSAM is to check that green and yellow frames are transported with the required performance in terms of *Frame Total Delay* (FTD), *Frame Delay Variation* (FDV), *Frame Loss Ratio* (FLR) and availability. The existence of a policing algorithm like the trTCM means that testing the ability of the network to discard non-conforming traffic is another important requirement for eSAM. Transmission of green traffic is verified by the CIR test and the performance test, transmission of the yellow traffic is checked with the EIR test and red (discarded) traffic is measured by the policing test. Finally, the *Information Rate* (IR) is measured in all CIR, EIR and policing tests for all traffic classes to make sure that the information is preserved by the network when required to do so. More details about these specific tests are provided in the following sections.



Results-> Port B/eSAM/eSAM Configuration test

eSAM EIR test   Service 1/1 (PASS)

Color	IR (Mbit/s)	FLR	FTD (ms)	FDV (µs)
Green	100.000	0.000E+00	0.047	0
Yellow	20.008	5.998E-01	0.047	0
Total	120.008	1.999E-01	0.047	0

Results-> Port B/eSAM/eSAM Configuration test

eSAM Policing test   Service 1/1 (PASS)

Color	IR (Mbit/s)	FLR	FTD (ms)	FDV (µs)
Green	100.000	0.000E+00	0.047	0
Yellow	20.008	6.799E-01	0.047	0
Total	120.008	2.615E-01	0.047	0

Figure 7.9: EIR and policing test results as presented by Tempo.

7.2.2. Test Configuration

The way the equipment is configured depends on the particular network and service to be tested. Before running the test, there are several questions the user must answer:

- What kind of network is going to be tested? Configuration is different for IP networks and Ethernet networks. Note than a network may carry IP over Ethernet frames but it may still be more interesting to run an Ethernet test than an IPtest.
- How is the test equipment going to be connected to the network? Configuration is not the same if there is a traffic reflector used to loop frames back to the analyser (two-way test) or if *Port B* is going to be used for analysis (one-waytest).
- How many services are required to be measured in the same test? Is there any color marker used to classify the traffic? Which are the CIR / EIR values for each service? Is there any policing mechanism for the Ethernet services configured in the network?
- What is the required performance for each service in terms of FTD, FDV, FLR and availability?
- In IP tests, what are the correct IP profiles to be used? IP addresses, network masks, gateways and DNS servers (if used) must be known before the test can be configured. Usually DHCP protocol makes easier configuration of IP profiles but DHCP may not be available in some networks.

Table 7.8: eSAM Configuration

Setting	Description
Color mode	Set this field to *On* if the traffic contains color labels. Color labels enable the network to supply differentiated services to selected traffic. These services consist in low delay paths, high priority frame scheduling or low packet loss probability. Set the *Color mode* to *Off* if you want to leave the service provider network to decide the priority of user traffic based on the result of a traffic acceptance algorithm (policer, shaper).

Table 7.8: eSAM Configuration

Setting	Description
Color method	The color method configures which field in the test traffic implements the color mechanism. There are the following potential choices: • *DSCP*: Differentiated Services Code Point. It is 6-bit class of service label that accepts values between 0 and 63. DSCP makes sense as a color marker in routed networks and for this reason it is not available in *Ethernet endpoint mode*. • *C-VLAN priority*: 3-bit class of service field carried by the VLAN tag in IEEE 802.1Q frames or in the C-VLAN tag in IEEE 802.1ad and Q-in-Q frames. Using this field requires frames containing at least one VLAN tag. Color markers based on the C-VLAN priority field make sense only in switched networks for this reason it is not available in *IP Endpoint*. • *C-VID*: VLAN identifier assigned to tagged frames (IEEE 802.1Q) or C-VLAN identifier for double tagged frames (IEEE 802.1ad, Q-in-Q). The VID is commonly used in carrier Ethernet networks as a service discriminator. The test unit accounts for the possibility to use this field as a color marker as well. It requires the tester to be configured in *Ethernet Endpoint* mode and an encapsulation with at least one VLAN tag. • *S-VLAN priority*: 3-bit class of service field carried by the S-VLAN tag in IEEE 802.1ad and Q-in-Q frames. Color markers based on the C-VLAN priority field make sense only in switched networks for this reason it is not available i*n IP Endpoint* mode. • *S-VID*: VLAN identifier assigned S-VLAN tag in double tagged frames (IEEE 802.1ad, Q-in-Q). The VID is commonly used in carrier Ethernet networks as a service discriminator. The test unit accounts for the possibility to use this field as a color marker as well. It requires the tester to be configured in *Ethernet Endpoint* mode and an IEEE 802.1ad / Q-in-Q encapsulation
Number of services	Defines the number of services to be simultaneously tested. The maximum number of services to be tested is eight (non- color-aware mode) or four (color-aware mode).

Table 7.8: eSAM Configuration

Setting	Description
Number of steps	Number of different bit rates to be tested in the configuration CIR test. The test bit rates are equally distributed between 0 and CIR bit rates.
Step duration (s)	Duration of each iteration of the CIR test. If Number of steps is configured to 1, it is the duration of the CIR test. Any value between 1 and 60 seconds is accepted.
Policing test	Enable to execute the policing test as a part of the eSAM test suite or disable if you don't want to run the policing test. You may want to disable the policing test if you know that the network under test is not using any traffic admission algorithm and you don't want the configuration test to fail for this reason.
Performance test duration	Duration of the eSAM performance test. The performance test is executed once the configuration test has finished. For the performance test you can choose between one of the three duration presets (*15 min.*, *2 hours*, *24 hours*) or you can set your own test duration with a resolution of one second by setting this field to *User duration*. It is possible to use this field to disable the performance test. This is interesting if you want to check the network configuration but you don't need to know the performance.
User duration	Use this field to configure the eSAM performance testduration if you have set *Performance test duration* to *User duration*.
Service configuration	Displays a panel that enables the user to enter the CIR and EIR for each service to be tested. The service configuration panel also displays information about traffic flows assigned to each eSAM service. Two flows are required to test one color-aware service and one flow is necessary for each non-color-aware service.

Once all the details about test equipment connection and network / service configuration have been clarified is time to configure the test. To do that follow these steps:

1. Make sure that your tester is connected to the network. The physical layer must be up and working (See section 4.1.1).
2. From the *Home* panel, go to *CONFIG*,
   The port setup panel is displayed.

3. Choose between *Ethernet endpoint* or *IP endpoint* with the *Mode* setting.
4. From the *Home* panel, go to *TEST*,
   The test configuration panel is displayed.
5. Go to *Performance test* and configure *eSAM*.
6. Enter in the *eSAM* menu to configure the global ITU-T Y.1564 settings.
7. Configure the *Color mode* to *On* if the service provider allows pre-marking of Ethernet frames / IP datagrams or set it to *Off* otherwise.
8. If you have configured *Color mode* to *On*, set the *Color method* to *DSCP* (IP Endpoint mode), *C-VLAN priority*, *C-VID*, *S-VLAN priority* or *S-VID* (Ethernet Endpoint mode).
   Note: C-VLAN priority and C-VID color markers require VLAN, Q-in-Q or IEEE 802.1ad encapsulation. S-VLAN priority and S-VID color markers require Q-in-Q or IEEE 802.1ad encapsulation.
9. Set the number of services you want to test within the same test with the help of the *Number of services* control.
   Note: The maximum number of services is 4 if *Color mode* is *On* or 8 if *Color mode* has been configured to *Off*.
10. Configure the *CIR* and *EIR* parameters for each service to be tested from the *Service configuration* panel.
11. Enter the number of steps and duration of each step for the CIR test with the help of the *Number of steps* and *Step duration (s)* controls.

Table 7.9: eSAM Performance Metrics

Result	Description
Load (Mbit/s)	Amount of test traffic offered to the network expressed in Mbit/s. This traffic is always larger or equal than the measured *Information Rate* (IR). Currently this parameter is displayed as a result only for the CIR configuration test. Traffic load for EIR and performance tests can be checked in the service configuration panel for eSAM tests. For policing tests, the load is always higher than the CIR + EIR in an amount than is computed automatically as specified in ITU-T Y.1564.
IR (Mbit/s)	Average *Information Rate* (IR) computed for the traffic currently being tested (green, yellow, aggregated, etc.) within the configured test period. Only test traffic is taken into account to measure the IR. The definition and application of the IR metric follows ITU-T Y.1564.

Table 7.9: eSAM Performance Metrics

Result	Description
FLR	Ratio of the total amount of lost frames to the total transmitted frames from the beginning of the test. Definition of the FLR parameter follows ITU-T Y.1563.
FTD (ms)	Is the worst case (maximum) *Frame Total Delay* (FTD) found from the beginning of the eSAM configuration or performance test and expressed in milliseconds. The definition of *FTD (ms)* follows ITU-T Y.1563 and it is computed in the same way that the *FTD (maximum)* metric supplied by the Tempo *SLA statistics*.
FDV (ms)	Is the worst case (maximum) *Frame Delay Variation* (FDV) found from the beginning of the eSAM configuration orperformance test and expressed in millisecond. The definition of *FDV (ms)* follows RFC 3393 and RFC 1889 and it is computed in the same way that the *FDV (maximum)* metric supplied by the Tempo *SLA statistics*.
Avail (%)	The Avail (%) constitutes an availability performance figure that informs about the percentage of time that the DUT / SUT has been not available for transmit / receive data during the eSAM performance test. This performance metric is computed as *100% - PEU(%)*. Where the PEU(%) is the Percent Ethernet service Unavailability defined in ITU-T Y.1563 and supplied by the Tempo *SLA statistics*. This metric is computed for eSAM performance tests only. Configuration tests are considered too short to make any accurate availability result significant enough.

12. Enable the policing test with *Policing test* if your network is using a traffic admission mechanism that limits the amount of accepted ingress traffic.
13. Configure the duration of the eSAM performance test with the help of the *Performance test duration* and *User duration* controls.
14. Leave the *eSAM* configuration panel and from the *Test* menu select Performance objectives.
15. Select *eSAM* and enter the performance objectives in terms of the *FLR*, *FTD*, *FDV* and *Avail.* fields for each service you want to test.
16. Leave the *eSAM objectives* and *Performance test* panels.
17. Go to *Test mode.*

18. Depending on your test setup (See section 2.2.3), configure *Test method* to *One-way (A > B)*, *Two-way (A > A)*, *Upstream* or *Downstream*.
19. If you have configured either the *Upstream* or *Downstream* test modes, configure *Remote unit MAC* (in *Ethernet endpoint* mode) or *Remote unit IP* (in I*P endpoint* mode).
    Note: A unit configured in *Remotely managed* mode has to be installed and configured in the remote end before any asymmetric test can be run (See section 7.4).
20. From the *Home* panel, go to *CONFIG*,
    The port setup panel is displayed.
21. Configure the *Frame layer* (See section 4.1.2) in Port A for all your services. Parameters to be configured are source and destination MAC addresses, VLANs, frame size, etc.
    Note: To know the correspondence between flows and eSAM services, check the *Service configuration* panel you have used to configure the CIR and EIR values for the test.
    Note: Test traffic corresponding to different services should not have exact configurations. Otherwise, the analyser (and the network) will fail to classify the traffic. A service delimiting field could be used for this purpose. It is common to use the VID but anything that makes traffic from different services different in some way is accepted by the tester.
    Note: If you are configuring coloured traffic, the color markers (C-VLAN priority, C-VID, S-VLAN priority, S-VID) must have a different value for green and yellow traffic corresponding to the same service. The test will fail to start if this requirement is not met.
    Note: If you are running an *Upstream* asymmetric test in *Ethernet endpoint* mode, you are allowed to configure the *Destination MAC address from* field to *Remote*. In this way, you are setting the destination MAC address to be the responder address.
    Note: If you are running a *Downstream* asymmetric test, you need to think in the port settings you configure as the configuration for the responder device (who is going to be the traffic generator). For this reason you are allowed to configure the *Source MAC address from* field to *Remote*. This setting configures the source address in the traffic generator (the responder device, in this mode) to be the own responder address.
22. If you are working in *IP endpoint* mode, configure the *Local profile* (See section 2.3) and the *Network layer* (See section 4.2.4) for all your services. Parameters to be configured are IP addresses, DSCPs, etc.
    Note: Previous notes about flows / services, service delimiting tags and color markers are valid in *IP endpoint* as well but in this case the color marker to be used is the DSCP rather than VLAN priorities or VIDs.
    Note: If you are running an *Upstream* asymmetric test in *IP endpoint* mode, you are allowed to configure the *Destination IP address from* field to *Remote*. In this way, you are setting the destination IP address to be the responder address.

Note: In the same way than in *Downstream* Ethernet end point tests, you need to think in the port settings you configure as the configuration for the responder device. For this reason you are allowed to configure the *Source IP address from* field to *Remote*. This setting configures the source address in the traffic generator to be the own responder IP address.

23. Run the eSAM test with the help of the *run* button.

You can optionally attach a GNSS receiver to the test units (controller and responder) to measure one way delay in the eSAM test (See section 2.6.2). To do that follow these steps:

1. From the *Home* panel, go to *CONFIG*,
   The port setup panel is displayed.
2. Go to Reference clock.
3. Configure Input clock to GNSS.

7.2.3. CIR Configuration Test

The CIR Configuration test is the most basic eSAM test. Its purpose is to check the ability of the network to deliver frames at CIR rate within acceptable performance limits. This test consist in loading the service with the maximum bit rate it supports without any degradation that is the CIR by definition. Optionally, the user is allowed to configure other test rates smaller than the CIR. For colored services, the only traffic color to be generated in the CIR test is green.

CIR test results are made up of the IR, FTD, FDV and FLR for all the test loads. The test is considered to pass if the computed performance metrics (FTD, FDV and FLR) are better than the corresponding performance thresholds. Test results, including the final Pass / Fail are essentially the same for color aware and non-color aware CIR tests.

It is possible to execute several (up to four color-aware or eight non-color-aware) CIR tests. In this case, CIR tests are executed sequentially for each configured service. To check the CIR test results follow this procedure:

1. From the *Home* panel, go to *RESULTS*,
   The test port results panel is displayed.
2. Select either *Port A or Port B* to enter in the port specific results.
   Note: If you have configured *Test method* to *One-way (A > B),* the eSAM results are available in *Port B*. On the other hand, if you have configured *Two-way (A > A), Upstream* or *Downstream*, the eSAM results are available in *Port A*.
3. Select *eSAM*.
4. Check the *Status* field to know the pass / fail test result. If the test has not yet finished, this field will display a *In progress* message. If the equipment detects an error during text execution it will display an error message.
5. Check the *Test remaining time* to get an estimation about how much time is left to finish the current test.

6. Go to *eSAM Configuration test*.
   A table with eSAM configuration test results is displayed.
7. Use the *Test-* and *Test+* contextual keys to select the eSAM CIR test results. Use the *Serv-* and *Serv+* contextual keys to select the table corresponding to the service you want to check.

7.2.4. EIR Configuration Test

The purpose of the EIR Configuration test is to measure network performance when it is loaded with an information rate that matches the CIR + EIR. Unlike it happens with the CIR configuration test, the way the results are computed is very different for color-aware and non-color-aware services. The reason is that there is no performance limit in non-color-aware services when the transmission rate is above the CIR but for color-aware services it is still possible to guarantee the quality of service of green frames. The EIR test is executed and evaluated as follows:

- *Non-color-aware services*: The network is loaded with a CIR + EIR bit rate and the IR, FTD, FDV and FLR are measured. The test is considered to pass if CIR * (1 - FLR) < IR < CIR + EIR.
- *Color-aware services*: The network is loaded with CIR green traffic and EIR yellow traffic. The IR, FTD, FDV and FLR is measured for both traffic classes. The test is passed if the FTD, FDV and FLR for green traffic are within acceptable limits.

It must be noticed that performance metrics are always measured but they are relevant for the pass / fail results only for guaranteed (green) traffic.

It is possible to execute several (up to four color-aware or eight non-color-aware) EIR tests. In this case, EIR tests are executed sequentially for each configured service. Users may not want to run the EIR test. To do that, they have simply to configure the EIR to 0 for services where the test is not going to be executed.

The procedure to follow to display the EIR test results is similar than for the CIR results but in this case it is necessary to use he *Test-* and *Test+* contextual keys to select the eSAM EIR test results rather than the CIR ones

7.2.5. Policing Configuration Test

The Policing test is useful to make sure that the network drops non-conforming (red) traffic. The policing test loads the network with a policing rate computed automatically as specified in ITU-T Y.1564. The policing test is always higher than the sum of the CIR and the EIR. Again, test execution and result presentation is different in color-aware and non-color aware services. Details are as follows:

- *Non color-aware services*: The network is loaded with a CIR + EIR + policing bit rate and the IR, FTD, FDV and FLR are measured. The test is considered to pass if CIR * (1 - FLR) < IR < CIR + EIR + 1%. The extra 1% is used to account for the burstability of policing filters due to an EBS parameter different to zero.
- *Color-aware services*: The network is loaded with CIR green traffic and EIR + policing yellow traffic. The IR, FTD, FDV and FLR is measured for both traffic

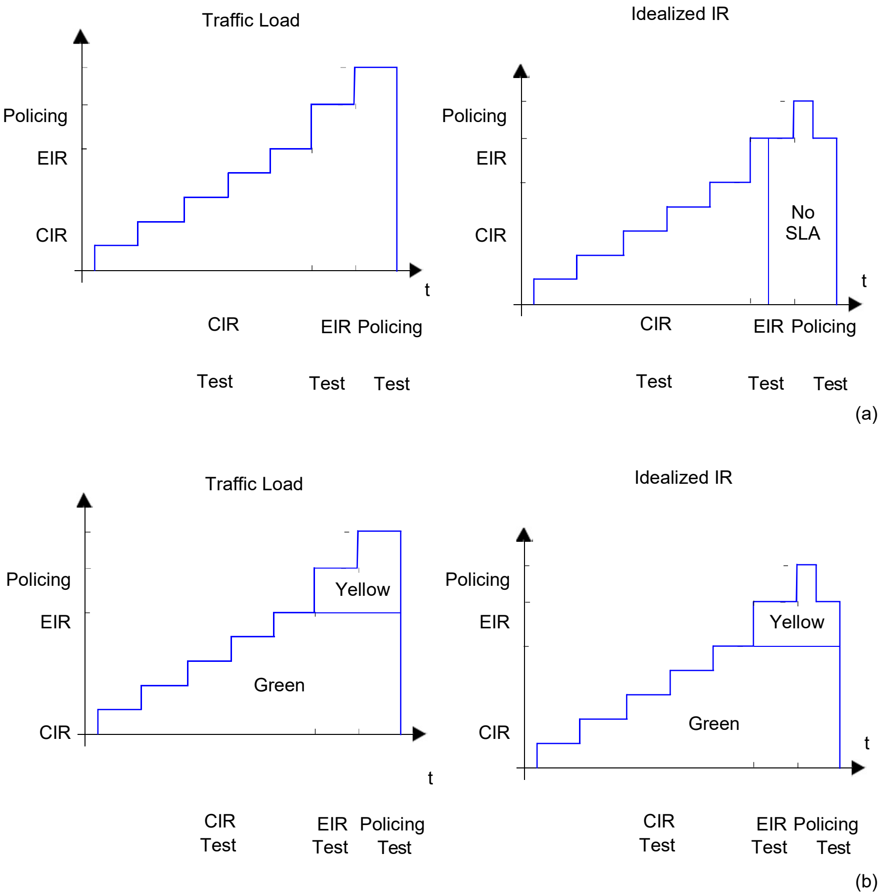


Figure 7.10: Typical CIR, EIR and Policing tests in colour-aware and non colour aware services: (a) No colours are defined in the interface. Some traffic may be degraded if CIR < IR < EIR because quality of service is not guaranteed for excess traffic. If IR > EIR some traffic will be lost due to the action of the policing filter. (b) Coloured interface: Yellow traffic does not have quality of service guarantees but SLA is meet for Green traffic as long as the IR remains smaller than the CIR.

classes. The test is passed if the FTD, FDV and FLR for green traffic are within acceptable limits and if the aggregated IR (green + yellow) meets the following double inequality: CIR * (1 - FLR) < IR < CIR + EIR + 1%.

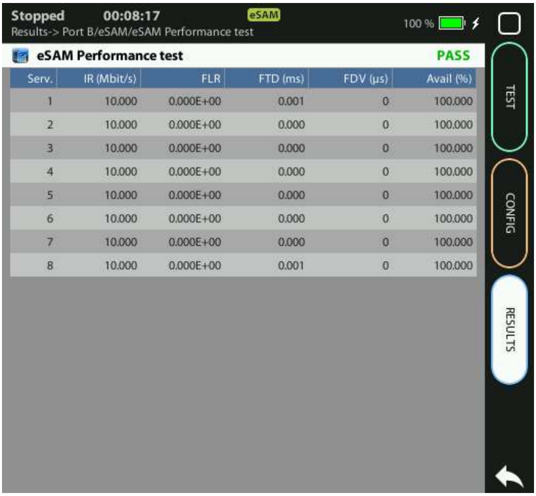
Like it happens with the CIR and EIR tests, it is possible to execute several (up to four color-aware or eight non-color-aware) policing tests. In this case, policing tests are executed sequentially for each configured service.

Users may choose to disable the policing test if the network is not using any admission control mechanism based on policing filters. The policing test fails if it is executed in networks not supporting policing.

The procedure to follow to display the policing test results is similar than for the CIR results but in this case it is necessary to use he *Test-* and *Test+* contextual keys to select the eSAM policing test results rather than the CIR ones

7.2.6. Performance Test

The eSAM performance test is executed only if the configuration CIR, EIR and policing tests are passed. While configuration tests take a few minutes to finish, a performance test may take hours or even days depending on the test requirements.



Stopped 00:08:17 eSAM

Results-> Port B/eSAM/eSAM Performance test

100 %

eSAM Performance test PASS

Serv.	IR (Mbit/s)	FLR	FTD (ms)	FDV (µs)	Avail (%)
1	10.000	0.000E+00	0.001	0	100.000
2	10.000	0.000E+00	0.000	0	100.000
3	10.000	0.000E+00	0.000	0	100.000
4	10.000	0.000E+00	0.000	0	100.000
5	10.000	0.000E+00	0.000	0	100.000
6	10.000	0.000E+00	0.000	0	100.000
7	10.000	0.000E+00	0.000	0	100.000
8	10.000	0.000E+00	0.001	0	100.000

Figure 7.11: Performance results as presented by Tempo.

In some ways, the performance test is similar to the CIR test because in the network is loaded with the CIR bit rates of all configured service but in this case all services are tested simultaneously and therefore the total load is the sum of all CIR rates for all Ethernet services under test. This is important because a network may be able to support all services if they are not all them loaded at the same time but it may fail to support all services operating at maximum speed. The second difference between CIR and performance tests is that performance test uses to be long enough to compute a significant availability figure.

The performance test computes the IR, FTD, FDV, FLR and availability for all the services being tested. The test is passed if all performance metrics are found to be within acceptable limits.

The procedure to follow to display the performance test results is similar than for the CIR results but in this case it is necessary to go the *eSAM Performance test* result panel rather than to the *eSAM Configuration test* panel.

7.2.7. Generation of eSAM Result Reports

Report generation for eSAM works in a similar way that for RFC 2544. There's no need to make any special configuration in order to get the eSAM test report. It is only necessary to enable report generation (See section 12.1).

Report organization is similar than in other tests, The report contains a header, containing details about which equipment has been used to run the test, when the tester has been executed, and other information, a global Pass / Fail indication, followed by test-specific Pass / Fail indications, a summary of the test setup and finally detailed descriptions of the eSAM configuration and performance tests.

```
eSAM test report

Report name              2013-04-11-173048
Custom
Department
Company
Location
Operator
Start Time               Thu Apr 11 17:30:48 2013
Elapsed Time             00:03:08
Test Unit                Ether.Giga Gigabit Ethernet Tester
Serial number            MEM0009P
Software version         1.13.35


Global results (Port A)

                                   Service         Status

Global status                          ---           PASS

eSAM Configuration test                  1           PASS
eSAM Configuration test                  2           PASS
eSAM Configuration test                  3           PASS
eSAM Configuration test                  4           PASS
eSAM Performance test                  ---           PASS


Test Unit Configuration

Mode                                     IP endpoint
Test method                              Two-way (A > A)

                                         Port A              Port B
Port mode                                TX/RX               Loopback
Connector                                Electrical          Optical

eSAM test configuration

Color mode                                            On
Color method                                        DSCP
```

```
Number of services                                      4
Number of steps                                         1
Step duration (s)                                       3
Policing test                                    Disabled
Performance test duration                   User duration
User duration                                    00:01:00


Service configuration

Service                CIR            EIR
   1           2.000 Mb/s     2.000 Mb/s
   2           2.000 Mb/s     2.000 Mb/s
   3           2.500 Mb/s     2.500 Mb/s
   4           2.500 Mb/s     2.500 Mb/s


eSAM objectives

Service                FLR            FTD            FDV          Avail.
   1            1.000E-03     100.000 ms      50.000 ms        99.000 %
   2            1.000E-03     100.000 ms      50.000 ms        99.000 %
   3            1.000E-03     100.000 ms      50.000 ms        99.000 %
   4            1.000E-03     100.000 ms      50.000 ms        99.000 %

eSAM CIR test

Service 1

Load (Mbit/s)    IR (Mbit/s)   FLR         FTD (ms)   FDV (ms)    Status
2.000            2.000        0.000E+00    0.145      0.014       PASS

Service 2

Load (Mbit/s)    IR (Mbit/s)   FLR         FTD (ms)   FDV (ms)    Status
2.000            2.000         0.000E+00   0.158      0.015       PASS

Service 3

Load (Mbit/s)    IR (Mbit/s)   FLR         FTD (ms)   FDV (ms)    Status
2.500            2.500         0.000E+00   0.149      0.022       PASS

Service 4

Load (Mbit/s)    IR (Mbit/s)   FLR         FTD (ms)  FDV (ms)     Status
2.500            2.500         0.000E+00   0.148     0.019        PASS

eSAM EIR test

Service 1

Color    IR (Mbit/s)          FLR       FTD (ms)        FDV (ms)     Status
Green          2.000    0.000E+00          0.395           0.115       PASS
Yellow         2.000    0.000E+00          0.388           0.116       PASS
Total          4.000    0.000E+00          0.395           0.116       PASS

Service 2

Color    IR (Mbit/s)          FLR       FTD (ms)        FDV (ms)     Status
Green          2.000    0.000E+00          0.141           0.012       PASS
Yellow         2.000    0.000E+00          0.144           0.012       PASS
Total          4.000    0.000E+00          0.144           0.012       PASS
```

```
Service 3

Color    IR (Mbit/s)          FLR       FTD (ms)       FDV (ms)    Status
Green          2.500    0.000E+00          0.498          0.184      PASS
Yellow         2.500    0.000E+00          0.495          0.181      PASS
Total          5.000    0.000E+00          0.498          0.184      PASS

Service 4

Color    IR (Mbit/s)          FLR       FTD (ms)       FDV (ms)    Status
Green          2.500    0.000E+00          0.196          0.020      PASS
Yellow         2.500    0.000E+00          0.219          0.021      PASS
Total          5.000    0.000E+00          0.219          0.021      PASS


eSAM Policing test

Service 1

Color    IR (Mbit/s)          FLR       FTD (ms)       FDV (ms)    Status
Green           ----          ---           ----           ----      ----
Yellow          ----          ---           ----           ----      ----
Total           ----          ---           ----           ----      ----

Service 2

Color    IR (Mbit/s)          FLR       FTD (ms)       FDV (ms)    Status
Green           ----          ---           ----           ----      ----
Yellow          ----          ---           ----           ----      ----
Total           ----          ---           ----           ----      ----

Service 3

Color    IR (Mbit/s)          FLR       FTD (ms)       FDV (ms)    Status
Green           ----          ---           ----           ----      ----
Yellow          ----          ---           ----           ----      ----
Total           ----          ---           ----           ----      ----

Service 4

Color    IR (Mbit/s)          FLR       FTD (ms)       FDV (ms)    Status
Green           ----          ---           ----           ----      ----
Yellow          ----          ---           ----           ----      ----
Total           ----          ---           ----           ----      ----

eSAM Performance test

Service  IR (Mbit/s)   FLR        FTD (ms)   FDV (ms)   Avail.    Status
1        2.000         0.000E+00    0.501    0.071     100.000 %    PASS
2        2.000         0.000E+00    0.540    0.061     100.000 %    PASS
3        2.500         0.000E+00    0.484    0.063     100.000 %    PASS
4        2.500         0.000E+00    0.532    0.075     100.000 %    PASS
```

7.3.Performance Assessment with the RFC 6349

Both the RFC 2544 and the eSAM tests are Ethernet and IP tests that provide the same result regardless of the application. They generate fixed frame rates and verify the ability of the network to transmit this traffic with a low impairment level.

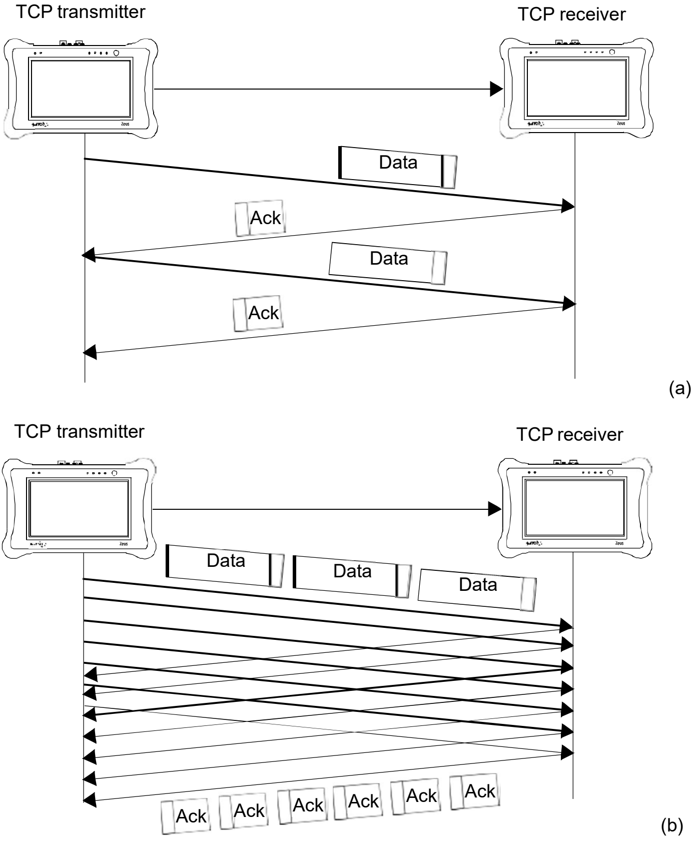


Figure 7.12: (a) No window is used: The transmitter has to wait for the acknowledge message to resume transmission. (b) TCP window mechanism: Continuous transmission can be achieved.

The RFC 2544 and eSAM approach is good for low latency applications (video, voice) based on the *User Datagram Protocol* (UDP) but it has proven to be insufficient for data transfer applications (web, file transfer, e-mail) which are highly sensitive to transmission errors and they are often based on the *Transmission Control Protocol* (TCP). TCP is more complex than UCP. Unlike UDP, TCP is connection oriented, which means that there are TCP handshaking and connection termination procedures. For this reason, TCP endpoints are required to keep status information about open connections. The entity that starts the communication by initiating the handshaking procedure is the TCP client. The TCP server, on the other hand, accepts connections from clients and responds to their queries while the connection is active

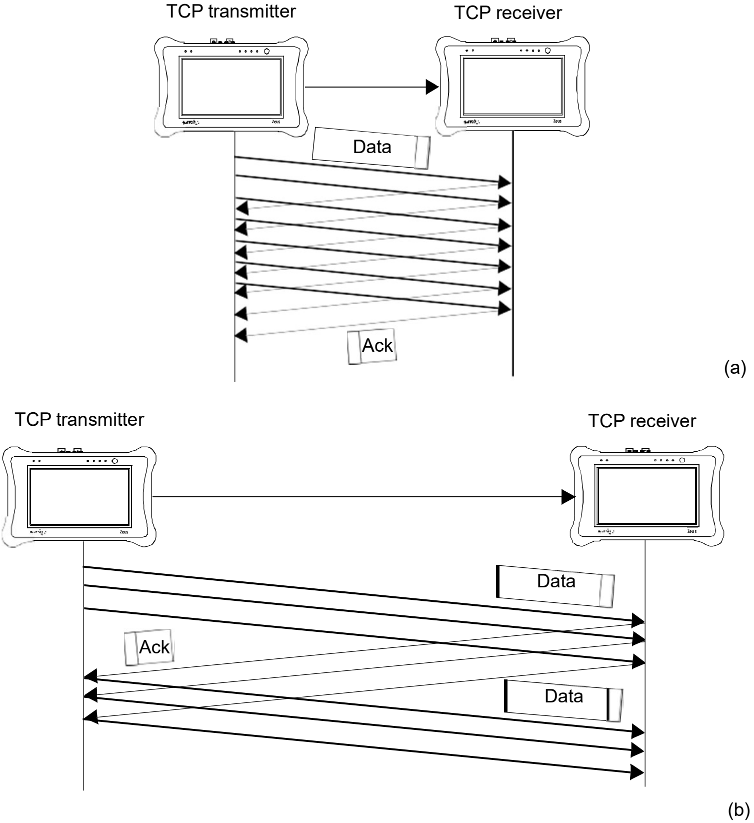


Figure 7.13: The importance of setting a correct window to achieve optimum performance in TCP data transfer: (a) The window is set to a value larger than the BDP and transmission is continuous. (b) If the window is smaller than the BDP the transmitter has to stop at some points and wait for acknowledge messages from the far end.

The mechanism that sets the UDP transmission rate is out of the scope of the protocol itself. The transmitter sets the speed to 100 kb/s, 1 Mb/s, 10 Mb/s or any value required by the application. If the network or the receiver is not able to process the traffic, they just start dropping packets. There is also no way to recover lost data unless a data recovery mechanism is implemented by the application. In TCP, the transmission speed is controlled by the receiver rather than the transmitter as in UDP. The TCP receiver controls which data is to be transmitted by generating acknowledge messages and the transmitter has to stop sending data if the previous messages have not been acknowledged. In order to increase the transmission efficiency, a sliding window mechanism is defined: The TCP transmitter is allowed to generate unacknowledged packets up to a certain limit specified by a window which is defined in terms of certain amount of data often expressed in KB. If the window mechanism is properly implemented, continuous transmission is achieved without the need to wait for each individual acknowledge message. The window mechanism is sensitive to network delay. If latency is increased beyond a limit, the transmitter does not have time to receive acknowledgement messages for transmitted data before the window is empty and it therefore must stop and wait. Something similar happens if the transmission speed increases because then the window empties faster. Given the transmission bandwidth and the *Round Trip Time* (RTT), there is a minimum window size that ensures that data transfer occurs without interruptions. This minimum window size is the *Bandwidth-Delay Product* (BDP). If the window size configured in the endpoint is smaller than the BDP, transmission will not achieve the optimum rate and the bandwidth will be partly wasted. For example, in a 1 Gb/s Ethernet path, with a delay (RTT) of 500 μs, the BDP is 61 KB. If the transmitter configures a transmission window of 16 KB, then the maximum achievable bandwidth will be 262 Mb/s.

The TCP sliding window mechanism allows the TCP to fill the line with a continuous data flow but it is also flexible enough to adapt the flow to varying transmission conditions. When used together with the Automatic Repeat Request (ARQ), the function that enables TCP to detect and re-transmit lost or corrupted data, the sliding window becomes also a congestion management mechanism that enables the transmitter to adjust the window size on detecting packet loss events in order to speed up or down data transfer. There are, actually, many different implementations of the TCP protocol. They differ on how they manage retransmission of lost / corrupted data, on congestion control and in other aspects. The Tempo test unit is based on a TCP implementation known as NewReno.

Despite offering potentially different performance levels, all TCP implementations are required to be inter-operable. One of the key aspects of compatibility between them is that they share the same segment structure, which is defined in RFC 793 and it was later complemented by RFC 3040 and RFC 3168. The TCP header is 20 bytes long when no options are appended to it. This length has to be taken into account when the transmission efficiency is rated. For example, in a 1 Gb/s Ethernet link, if TCP is transported over the IPv4 protocol, it achieves at most 949 Mb/s (1518 byte frames). This is because an Ethernet 1 Gb/s interface includes *Maximum Transmission Unit* (MTU) frames (1518 bytes), the preamble (8 bytes), and the *Interframe Gap* (IFG) (12 bytes), which totals 1536 bytes. However the TCP payload is the MTU minus the Ethernet header (14 bytes), the Ethernet *Frame Check Sequence* (FCS) (4 bytes), the IPv4 header (20 bytes) and the TCP header (20 bytes). Finally, only 1460 bytes are left for user data transmission. In a lossless (no retransmissions) channel, if the TCP sliding window mechanism is properly implemented, the transmission efficiency is the ratio between 1460 bytes and 1518 bytes, which accounts for 94.9% (949 Mb/s in a 1000 Mb/s link). In our previous example about transmission over a 1 Gb/s path with a delay of 500 μs and a window of 16 KB, the real transmission capacity must take into account the frame-to-payload ratio. The result is the product of 262 Mb/s and 94.9% which is only 249 Mb/s.

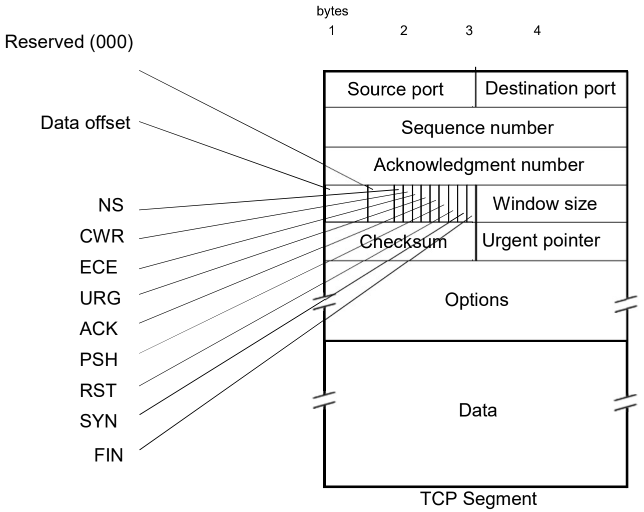


Figure 7.14: TCP segment structure

The previous examples have shown that incorrect TCP settings lead to drastic reduction of net transmission bandwidth. The purpose of the RFC 6349 is to help network administrators to deal with issues that are specific of TCP transmission.

The last point in this short introduction to TCP and the RFC 6349 remembers that this test alone may not be sufficient to provide an accurate diagnostic of the transmission performance and it is often required to run a complementary RFC 2544 or eSAM test before investigating the TCP throughput. Proceeding in this way is beneficial to detect potential issues in the data link and network layers before investigating the transfer layer

7.3.1. Configuring the RFC 6349 Test

Tempo has the ability to generate TCP flows to verify the protocol performance in terms of the metrics defined in standard RFC 6349. Users have control on how the TCP traffic is generated, the metrics to be evaluated and the performance thresholds required to declare a *Pass* or *Fail*.

The RFC 6349 test is made up of three different tests. These tests are described in the following list:

- *Baseline RTT test*: Measures the *baseline RTT,* the minimum time it takes for a TCP packet to travel from the near end to the far end and back to the near end. The baseline RTT could be also defined as the uncongested delay associated to the network under test. The test unit generates a low speed TCP connection to measure the baseline RTT a low speed TCP with the purpose of avoid network congestion. The baseline RTT test could be disabled by the user, which is then requested to configure this parameter manually.
- *Window sweep test*: Measures the TCP throughput for different window sizes smaller or equal to the BDP and compares the theoretical and actual results to detect potential issues.
- *TCP throughput test*: For the BDP window, it rates the TCP protocol in terms of Throughput, the transmission speed achieved during the test, the Efficiency, which is related with presence of lost messages and retransmissions and the buffer delay which accounts for the latency increase due to congestion.

Table 7.10: RFC 6349 Configuration

Setting	Description
Server TCP port	Configures the TCP server to listen from this port and the TCP client to generate traffic to this port (destination port in TCP is set to this value in traffic generated from the client). The default Server TCP port is 55220. You may want to change the port if you are not allowed to use the default value for any reason such as the presence of a firewall that blocks connections though certain ports or port ranges.
Path MTU	Longest packet that the network accepts without applying fragmentation.To account for the MTU size the Ethernet header, payload and FCS field are taken into account but the Preamble and IFG are not. The default MTU is 1518 bytes but values up to 10 KB are accepted. Modify the default MTU only if you know that the network accepts frames longer than the standard value.
Enable RTT test	Enables or disables the baseline RTT test. The baseline RTT is measured through a low speed TCP session generated by the test unit to avoid congesting the network and thus getting a good estimate of the baseline RTT.
User RTT	User configurable baseline RTT. If the uses disables the baseline RTT test through the *Enable RTT test* control, then it will be necessary to enter a user value expressed in micro-seconds.

Table 7.10: RFC 6349 Configuration

Setting	Description
RTT test duration	Configures the baseline RTT test duration. If *Enable RTT* test is configured to *Enabled*, then this field specifies the testing period for this parameter.
Enable window sweep test	Enables or disables the window sweep test. The window sweep test measures the transmission throughput for different window sizes and it
Step duration	Configures the measurement time for each iteration in the window sweep tests.
Throughput test duration	Duration of the RFC 6349 TCP throughput test. For the throughput test you can choose between one of the three duration presets (*15 min.*, *2 hours*, *24 hours*) or you can set your own test duration with a resolution of one second by setting this field to *User duration*.
User duration	Use this field to configure the RFC 6349 throughput test duration if you have set *Throughput test duration* to *User duration*.
Expected IR upstream	This field contains the upstream bandwidth configured in the test path or previously measured with the help the RFC 2544 test or other procedure. The test unit will use this value together with the baseline RTT to set the transmission window in the client-to-server direction. The *Expected IR upstream* is L1 bandwidth and therefore all Ethernet fields (header, payload and FCS), IFG and Preamble, are considered to be included. For example, in a 1 Gb/s Ethernet link with no constrains the Expected IR upstream is exactly 1 Gb/s.
Expected IR downstream	This field contains the downstream bandwidth configured in the test path or previously measured with the help the RFC 2544 test or other procedure. The test unit will use this value together with the baseline RTT to set the transmission window in the server-to-client direction. The *Expected IR upstream* is L1 bandwidth and therefore all Ethernet fields (header, payload and FCS), IFG and Preamble, are considered to be included. For example, in a 1 Gb/s Ethernet link with no constrains the Expected IR upstream is exactly 1 Gb/s.

Table 7.10: RFC 6349 Configuration

Setting	Description
Allow multiple connections	When enabled, the TCP test traffic is evenly shared between several TCP streams. This condition leads to a more realistic test conditions in many scenarios.
Preferred window size	The test engine attempts to use a window size as close as possible to the value configured by this setting. The actual window size may be different to the preferred window size when either the required number streams for the calculated BDP is either to small or too large to accomplish with this objective.
Maximum duration	This is a read only field that contains the maximum test duration based on the current settings.

To configure the TCP throughput test in Tempo, follow these steps:

1. Make sure that your tester is connected to the network. The physical layer must be up and working (See section 4.1.1).
   Note: If you plan to run a test between Port A and Port B within the same unit, then the physical layer must be up and working in both ports.
2. From the *Home* panel, go to *CONFIG*,
   The port setup panel is displayed.
3. Configure *IP endpoint* with the *Mode* setting.
4. From the *Home* panel, go to *TEST*,
   The test configuration panel is displayed.
5. Go to *Performance test* and configure *RFC 6349*.
6. Go to *RFC 6349 configuration*.
7. Optionally, configure the *Server TCP port* and the *Path MTU*.
8. If the baseline RTT is unknown, then configure *Enable RTT test* to *Enabled*. If the baseline RTT has been previously measured you can disable this test.
9. If you have enabled the baseline RTT test in the previous step, configure the test duration with the help of the *RTT test duration* control. If the baseline RTT test is disabled, then configure *User RTT* to the right value.
10. Enable or disable the window sweep test with the help of the *Enable window sweep test* field.
11. If you have enabled the window sweep test in the previous step, then configure *Step duration* to adjust the sweep test duration.
12. Configure the Expected IR upstream and Expected IR downstream in accordance with the test interface.
13. Optionally, enable *Allowed multiple connections* to measure throughput over more than one TCP stream.

14. If you have enabled Allow multiple connections in the previous stream, then set the *Preferred window size* for each TCP stream.
15. Leave the *RFC 6349 configuration* and *Performance test* panels.
16. Go to *Test mode*
17. Depending on your test setup (See section 7.4), configure *Test method* to *One-way (A > B)*, *Upstream*, *Downstream, Bidirectional* or *Local bidirectional*.
18. If you have configured any of the *Upstream, Downstream or Bidirectional* test modes, configure the *Remote unit IP*.
    Note: A unit configured in *Remotely managed* mode has to be installed and configured in the remote end before any dual ended test can run (See section 7.5).
19. From the *Home* panel, go to *CONFIG*,
    The port setup panel is displayed.
20. Go to *Port A*
21. Configure the Port A *Local profile* (See section 2.3).
22. If you are running a *Remote bidirectional* test the test configuration is ready. If you are running a *One-way (A > B)* or a *Local bidirectional* test, then leave *Port A* and go to *Port B.*
23. Configure the Port B *Local profile* (See section 2.3).

7.3.2. Setting the Performance Objectives

The TCP Throughput test based on the standard RFC 6349 provides results in terms of three different metrics: Throughput, Efficiency and Buffer delay. All three are described in the RFC 6349 standard:

- *Throughput*: Represents the maximum achievable bit rate between the client and the server entities (or between the server and the client). Only the TCP payload capacity is taken into account in this results. The Ethernet related fields (IFG, preamble, header, and FCS), IP header and TCP header are not taken into consideration. For this reason, the theoretical TCP throughput is smaller than the nominal L1 channel capacity. For example, a 1 Gb/s Ethernet, has a maximum TCP throughput of 949 Mb/s (1518 byte frames).
- *Efficiency*: It is defined as the ratio of successfully transmitted bytes to the total number of transmitted bytes. Efficiency decreases when data has to be retransmitted and the more retransmissions are necessary the smaller the TCP efficiency.This parameter is closely related with frame loss events.
- *Buffer delay*: This parameter is the ratio between the RTT computed during the throughput test and the inherent baseline RTT. This parameter is sensitive to waiting time in intermediate buffers and congestion.

The test unit provides a *Pass* or a *Fail* result for each of these parameters based on thresholds users can set at their will. The test unit provides one or two results for the throughput, efficiency and buffer delay depending on the test method (See section 7.4). One of the results correspond with the upstream and the other with the downstream. The thresholds apply to both of them.

To configure the RFC 6349 thresholds, follow these steps:

1. From the *Home* panel, go to *TEST*,
   The test configuration panel is displayed.
2. Go to *Performance test* and make sure that the *RFC 6349*.is configured.
3. Go to RFC 6349 objectives
4. Configure the value of *Minimum throughput*, *Minimum efficiency* and *Maximum buffer delay*.
   Note: You can set any of these values to 0 if you want them not to generate a Pass / Fail result and not to participate in the global RFC 6349 Pass / Fail result.

Table 7.11: RFC 6349 Performance Objectives

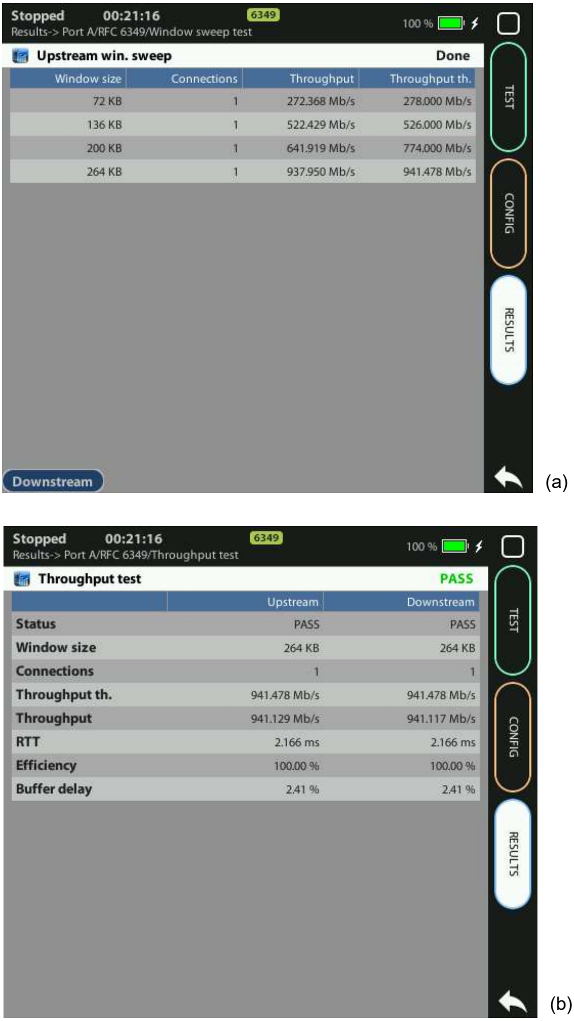
Setting	Description
Minimum throughput	Defines the minimum TCP throughput that generates a *Pass* result in the RFC 6349 throughput test. This threshold matches with both the *Upstream* and the *Downstream* TCP throughput and generates a *Fail* if any of these is smaller than the threshold. If the value of this field is set to zero then it will not be taken into account to generate the *Pass* / *Fail* result.
Minimum efficiency	Configures the minimum TCP efficiency that generates a *Pass* result in the RFC 6349 throughput test. This threshold matches with both the *Upstream* and the *Downstream Efficiency* result displayed in the *Throughput test* panel. If the value of this field is set to zero then it will not be taken into account to generate the *Pass* / *Fail* result.
Maximum buffer delay	Configures the maximum TCP buffer delay that generates a *Pass* result in the RFC 6349 throughput test. This threshold matches with both the *Upstream* and the *Downstream Buffer delay* result displayed in the *Throughput test* panel. If the value of this field is set to zero then it will not be taken into account to generate the *Pass* / *Fail* result.

7.3.3. Retrieving the Results

Once the RFC 6349 test has been configured and the performance objectives are adjusted, the test is ready to run. To start execution press *run* at any moment. You can wait to the end of the test do check the results but you can also get a partial view of these results during test execution. These are the steps required to and display results:

1. From the *Home* panel, go to *RESULTS*,
   The test port results panel is displayed.

2. Select *Port A* to enter in the port specific results.
3. Select *RFC 6349*.



(a)

Stopped 00:21:16 6349

Results-> Port A/RFC 6349/Window sweep test

100 %

Upstream win. sweep Done

Window size	Connections	Throughput	Throughput th.
72 KB	1	272.368 Mb/s	278.000 Mb/s
136 KB	1	522.429 Mb/s	526.000 Mb/s
200 KB	1	641.919 Mb/s	774.000 Mb/s
264 KB	1	937.950 Mb/s	941.478 Mb/s

(b)

Stopped 00:21:16 6349

Results-> Port A/RFC 6349/Throughput test

100 %

Throughput test PASS

	Upstream	Downstream
Status	PASS	PASS
Window size	264 KB	264 KB
Connections	1	1
Throughput th.	941.478 Mb/s	941.478 Mb/s
Throughput	941.129 Mb/s	941.117 Mb/s
RTT	2.166 ms	2.166 ms
Efficiency	100.00 %	100.00 %
Buffer delay	2.41 %	2.41 %

Figure 7.15: RFC 6349 results panels: (a) Window sweep test, (b) TCP throughput test.

4. Check the *Global status*, *Current test, Current test direction* and *Remaining* fields to get an overview of the current test status.

5. If you have enabled the baseline RTT test, go to *RTT test* to know the *Baseline RTT* and *Window size*.
6. If you have enabled the window sweep test, go to *Window sweep* and check the *Connections*, *Theoretical throughput* and *Throughput* for each transmission window.
7. Go to the *Throughput* test panel and check the *Status*, *Window size*, *Connections*, *Throughput*, *RTT*, *Efficiency* and *Buffer delay*.

Table 7.12: RFC 6349 Results

Setting	Description
Global status	Displays the current global test status. It can be any of the following: • *Aborted*: The test is terminated by the user either by pressing the *run* button or through the auto-start / stop function. • *Testing TCP connection*: A check procedure is running between the client and the server with the purpose to verify end-to-end connectivity between the near and the far end. Depending on the test method, these ends could be two ports of the same test unit. • *In progress*: The equipment is running any of the baseline RTT, window sweep or throughput tests. • *Error connect*: The unit fails to deliver TCP segments between the transmission ends. This message is usually displayed at the beginning of the test, when the TCP connection is verified but it can also happen at a later stage. • *PASS / FAIL*: Global result for the RFC 6349 test. The Pass or Fail indication is displayed at the end of the test depending on the result of comparing the TCP throughput, efficiency and buffer delay with their thresholds.
Current test	It either displays *Idle* if no test is running or an indication of the test that is being executed at the moment (*Round trip time*, *Window sweep*, *Throughput*).
Current test direction	Provides information about which transmission direction is currently under test (*Upstream* or *Downstream*). If no specific test duration is being tested then it displays *Idle*.
Remaining	Shows the estimated testing time based on the settings configured before the beginning of the tests.

Table 7.12: RFC 6349 Results

Setting	Description
RTT test	Menu that provides access to a panel with the baseline RTT test results if this test has been configured to run. This panel contains *Status* information (*Idle*, *In progress*, *Done*, *Error*), the *Baseline RTT* result and the *Window size* derived from the expected IR settings and the baseline RTT. This window size will be used to set a series of suboptimal test cases for the window sweep test and it will also be used to run the throughput test and compute the efficiency and latency results. The minimum allowed window size is 16 KB and starting from this, it can take only values that are multiples of 8 KB. If the BDPdoes not match with any of the allowed values then the window size is rounded to the closer upper allowed value. If you are running a bidirectional test, the RTT results panel will display information about each individual transmission directions.
Window sweep test	This is a menu that provides access to the window sweep results when this test has been configured to run. The window sweep result displays status information (*Idle*, *In progress*, *Done*, *Error*) and the results organized in a table where each row represents the results for one specifictransmission window. The results the test provides for each row are: • *Window size*: Window size used to generate TCP traffic in the current test iteration. It is always a fraction of the window size computed in the RTT test with the constrains of being at least 16 KB and being a multiple of 8 KB. • *Connections*: Number of concurrent TCP connections occurring in the current test iteration. It is always onefor the current RFC 6349 implementation. • *Theoretical throughput*: It is the throughput computed for the given window. It takes into account the potential throughput degradation derived from an incorrectwindow setting and the payload to frame length ratio for the TCP protocol and the configured MTU value. • *Throughput*: Measured TCP throughput for the given window. All Ethernet, IPv4 and TCP overhead is not taken into account for the throughput calculation. The measured throughput is always smaller or equal to the theoretical value.

Table 7.12: RFC 6349 Results

Setting	Description
Throughput test	Menu that provides access to the detailed TCP throughput results. The *Throughput test* panel provides *Status* information (*Idle*, *In progress*, *Done*, *Error*) and the following results: *Window size* derived from the BDP, *Connections*, *Throughput, RTT*, *Efficiency* and *Buffer delay*. In bidirectional tests two different results for each of these parameters one for the upstream and one for the downstream.

7.4. Configuring the Test Method

There are different ways to configure an automatic test depending on the location of the generator and the analyser and the data flow direction. If the generator and the analyser run in the same unit we speak about two-way or one-way tests but if hey are in different units then the test is asymmetric or remote. Depending on the test flow direction, tests could be upstream, downstream and bidirectional.

Table 7.13: Test Methods

	Upstream	Downstream
Generator and analyser in one unit	Local bidirectional Two way One way	Local bidirectional Two way
Distributed generator and analyser	Bidirectional Upstream	Bidirectional Downstream

Two-way tests measure network performance using a closed transmission path. There is usually a traffic reflector like Ether.Loop / Ether.DuaLoop / Ether10.DuaLoop that returns the traffic towards the origin. The return path is not always the same that the forward path but the test traffic always finishes in the same port where it was originated. Calnex test units support two-way tests in their Port A. Port B can be used as a local traffic reflector but installing an external reflector in a remote network location is also possible.

One-way tests are done in open paths in the network. Traffic is generated in a test interface, transmitted through the network and analysed by a second test port. Tempo supports one-way measurements between Port A and Port B in the same unit. In this way, it is guaranteed that the generator and the analyser are using the same timing source. Moreover, the test unit supports one.way latency measurements between two- units placed in remote locations with GNSS or 1 PPS / ToD synchronization.

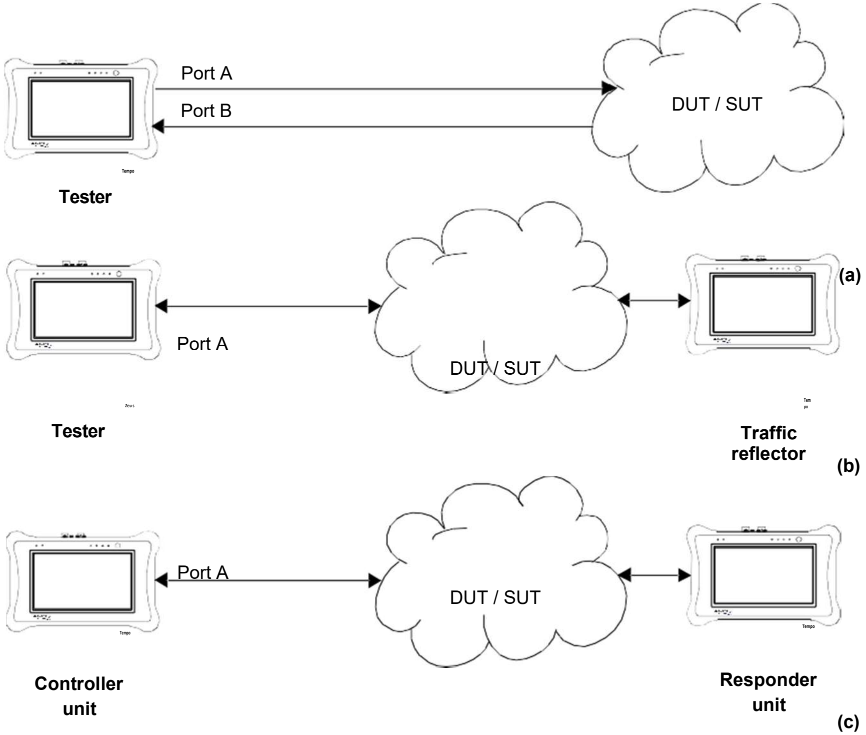


Figure 7.16: Connection setup for one-way and two-way tests: (a) One-way test, the test pattern leaves the tester in port A and it is received in port B. (b) Two-way test, the test pattern leaves in port A and it is received in the same port A (c) Asymmetric and bidirectional tests, the controller and responder units run a collaborative test. Typically, the controller generates commands for the responder. The responder executes these commands and it reports status and results.

The *Local bidirectional* test method is conceived as an extension to the *One-way* test but in a *Local bidirectional* test the traffic flows in both transmission directions. Unlike it happens with *One-way* tests, Local bidirectional tests run strictly between Port A and Port B within the same unit. Distributed test architectures are not supported when this test method is configured. The *Local bidirectional* test mode applies only to RFC 6349 tests.

The asymmetric test is also similar in some aspects to the one-way test method but it always requires two units to run. Asymmetric tests are more powerful than one-way tests because they allow the user to perform most of the configuration from a single end. Once finished, the results are shown in the same end where they were configured. The asymmetric test is based on collaborative operation of the controlling test unit and a remote responder unit (See section 7.5). The synchronization requirements are the same that in one-way tests running between two units. In latency measurements, the near and far ends require external synchronization. Asymmetric testing has to be supported by the particular test to be executed. Particularly, the asymmetric test is available in RFC 2544 and eSAM tests only (See section 7.1, See section 7.2).

Finally, the remote bidirectional test is similar to the asymmetric *Upstream* and *Downstream* methods but in the bidirectional test traffic flows between the controller and the responder. The remote bidirectional test applies only to RFC 6349 tests.

Table 7.14: Test Mode Configuration

Setting	Description
Remote managed	Enables or disables the responder operation in the unit. If this mode is enabled, most of the test unit functionality is controlled by a remote Calnex unit (See section 7.5).
Test method	Configures the way the currently configured test is to be executed. It is one of the following: • *One-way (A>B)*: Port A is configured for traffic generation. Port B becomes an analyser. This mode is suitable for measurements in open paths in the network and it is applicable to RFC 2544, eSAM and Y.1564 tests. • *Two-way (A>A)*: Port A is configured both for traffic generation and traffic analysis. This mode is suitable for measurements in closed paths in the network and it applies to RFC 2544 and eSAM tests. • *Upstream*: Configures the unit as a controller in an asymmetric test. The controller becomes a traffic generator and the responder an analyser. This test method is therefore suitable for the analysis of the path that goes from the controller to the responder. This test method is available only if one of the RFC 2544 or eSAM performance tests has been previously enabled. • *Downstream*: Configures the unit as a controller in an asymmetric test. The controller becomes a traffic analyser and the responder generates test traffic.This test method is therefore suitable for the analysis of the path that goes from the responder to the controller. This test method is available only if one of the RFC 2544 or eSAM performance tests has been previously enabled. • *Bidirectional*. Configures the unit as a controller in RFC 6349 dual-ended tests. The unit generates commands to control a remote unit running in responder mode and gets test results and status from the far end.

Table 7.14: Test Mode Configuration

Setting	Description
Test method	• *Local bidirectional*: Is a test method that runs between Port A and Port within the same test unit. In these tests both ports operate as traffic generators and analysers and therefore the test traffic runs in both transmission directions. The *Local bidirectional* test method applies to the RFC 6349 test only
Remote management UDP port	UDP port to be used for in-band signalling in asymmetric tests configured to run in IP endpoint mode. The in-band signalling generated in IP endpoint mode is made up of UDP packets. These packets are directed to the 55230 port. This port may be modified when required like in the case when the default port is blocked by a firewall. The in-band signalling in Ethernet endpoint is not encapsulated in UDP and port configuration is therefore not required.
Remote unit IP	Configures the responder IP address when the global operation mode is *IP endpoint* and *Test method* has been configured to either *Upstream* or *Downstream*. The responder global operation mode has to be configured to *IP endpoint* as well and the *Test mode* must be *Remotely managed*.
Remote unit MAC	Configures the responder MAC address when the global operation mode is *Ethernet endpoin*t and *Test method* has been configured to either *Upstream* or *Downstream*. The responder global operation mode has to be configured to *Ethernet endpoint* as well and the Test mode must be *Remotely managed*.
Remote test protocol status	This is a read only field that displays information about the responder from the controlling unit. The different possibilities are listed below: • *Idle*: The controller is not connected to the remote unit. This is the case when the test has not been started. • *Connected*: The controller is connected to the remote unit and running a test. This status is achieved once the user starts the test with the help of the *RUN* key or any other procedure. • *Agent unreachable*: The controller cannot connect to the remote unit. This situation arises either if there is a communication problem between the controller and the responder or when the controller / responder units arenot correctly configured.

Table 7.14: Test Mode Configuration

Setting	Description
Connected unit IP	This is a read only field that displays the IP address of any controller connected to a responder.This field makes sense only when the *Test method* is configured to *Remotely managed* and the global operation mode is *IP endpoint*.
Connected unit MAC	This is a read only field that displays the MAC address of any controller connected to a responder.This field makes sense only when the *Test method* is configured to *Remotely managed* and the global operation mode is *Ethernet endpoint*.

To configure the test method in your test unit, follow these steps:

1. From the *Home* panel, go to *TEST*,
   The test configuration panel is displayed.
2. Go to *Test mode*
3. Configure *Test method* to *One-way (A > B)*, *Two-way (A > A)*, *Upstream*, *Downstream, Local bidirectional* or *Remote bidirectional*.
   Note: The asymmetric test modes (*Upstream*, *Downstream*) are available only if an eSAM or RFC 2544 test has been previously enabled (See section 7.1, See section 7.2). The *Local bidirectional* and *Remote bidirectional* require the RFC 6349 (See section 7.3).
4. If you have configured either the *Upstream* or *Downstream* test modes, configure *Remote unit MAC* (in *Ethernet endpoint* mode) or *Remote unit IP* (in I*P endpoint* mode). If you have configured the *Remote bidirectional* test method, configure the *Remote unit IP*.
   Note: A unit configured in *Remotely managed* mode has to be installed and configured in the remote end before any asymmetric or remote bidirectional test can run (See section 7.5).

7.5. Using the Responder Function

Tempo can be remotely managed by a compatible test unit in order to run the RFC 2544 or ITU-T Y.1564 asymmetric tests and the RFC 6349 remote bidirectional test. The asymmetric tests are far more powerful than the symmetric RFC 2544 and ITU-T Y.1564 because they enable separated measurement of the upstream and the downstream. This is important in asymmetric paths, where each transmission direction has a different bandwidth, latency, etc. On the other hand, the remote bidirectional test is the only dual-ended test mode for RFC 6349 and it is mandatory to configure this mode whenever the test must between to geographically different locations.

When configured in responder mode, the unit becomes basically a passive device. All the instructions about how to run the test are generated by the remote unit and delivered to the test unit through an in band signalling channel. When a downstream test is configured in the remote unit, the responder acts as a traffic generator and the analysis is carried out in the far end. In the upstream test it happens the opposite: The responder analyses the traffic from the remote end and reports the result to the controller through the signalling channel. In bidirectional tests, the responder is at the same time a traffic generator and a traffic analyser. The correct procedure to configure Tempo as a passive responder is as follows:

1. From the *Home* panel, go to *CONFIG*,
   The port setup panel is displayed.
2. Select *Mode* to enter in the mode selection menu
3. Choose between: *Ethernet endpoint* or *IP endpoint*
   Note: This is an important decision. Controllers can connect only to responders configured to the same global operation mode.
   Note: Some tests may have more specific requirements. For example the Ethernet endpoint mode is not allowed by RFC 6349 tests
4. From the *Home* panel, go to *TEST*,
   The test setup panel is displayed.
5. Go to *Test mode*
6. Configure *Remotely managed*. to *Yes*.
   Note: Most functionality is disabled in remotely managed mode. The way to recover the unit whole compatibility is to disable this mode.
7. Wait for remote connections in Port A. These are signalled in the *Connected unit MAC* (Ethernet endpoint mode) or *Connected unit IP* (IP endpoint mode).

Chapter 8
Ping and Traceroute Tools

Ping and Traceroute are two basic IP network verification tools. Both Ping and Traceroute can be considered as an integrating part of the Operations, Administration and Maintenance (OAM) suite for the IP protocol family. Due to the high availability of this tools, Ping and Traceroute can be used for testing in almost any network.

8.1. Ping

Ping checks “distance” to any host in the network in terms of delay and packet loss. Results may not be as accurate as the SLA statistics supplied by other Tempo tests but Ping tests are fast, virtually supported by any IP network element and they are at least a good way to check end-to-end network connectivity before running a more sophisticated test.

8.1.1. Internet Control Message Protocol

Ping is an application of the *Internet Control Message Protocol* (ICMP) Echo request and Echo reply messages. The IP protocol alone is unable to monitor whether the packets arrive to final destination. Moreover, it does not provide any error reporting when routing and forwarding anomalies occur. This task is left to the ICMP protocol.

ICMP is a network layer Internet protocol that provides mechanisms to report errors and other information regarding IP packet processing back to the source. It is used for error reporting and analysis, transferring messages from routers and stations, and for reporting network configuration and performance problems.

ICMP generates several kinds of useful messages, including *Destination Unreachable*, *Echo Request* and *Echo Reply*, *Redirect*, *Time Exceeded*, and *Router Advertisement* and *Router Solicitation*. The ICMP functionality includes: Report network errors, Congestion indication, Troubleshooting assistance, Announce packet time-outs when TTL field is set to zero.

8.1.2. Test Configuration

The setup of a Ping test is much more simple than other tests. It does not require any special remote device like a traffic reflector to work and it works in virtually any network. The steps to follow to configure the IP ping are:

1. Make sure that the Port A of your tester is connected to the network. The physical layer must be up and working (See section 4.1.1).
2. From the *Home* panel, go to *CONFIG*
   The test port settings panel is displayed.
3. Configure *IP endpoint* with the help of the *Mode* setting.
4. Go to the *TEST* tab,
   The test configuration panel is displayed.
5. Configure *Ping/Traceroute* to *Ping*.
6. Go to the *CONFIG* tab
   The test port settings panel is displayed.
7. Select *Port A* to enter in the port A specific configuration.
8. Configure the *Local profile* (See section 2.3) either by means the DHCP protocol or by hand.
9. Go to *Ping/Traceroute*
10. Enter the destination IPv4 address by using the *Destination IPv4 address from*, *Destination IPv4 address* and *Destination host name*.
11. Configure the *Timeout*, *Interval*, *ICMP packet size* and *TTL* parameters for the test.
12. Run the Ping test with the help of *Run*.

Table 8.1: IP Ping Settings

Setting	Description
Destination IPv4 address from	Establishes the origin of the destination IPv4 address for the current stream. There are two different settings available for configuration: • *Manual*: The destination address is set to the value configured in *Destination IPv4 address*. • *Host name*: Uses the Domain Name Service (DNS) to set the destination IP address by using descriptive alphanumeric strings. The DNS mechanism requires intervention of at least one DNS server. The DNS server IP address has to be configured in the local port profile either statically or by means DHCP.

Table 8.1: IP Ping Settings

Setting	Description
Destination IPv4 address	Destination IPv4 address carried by the packets generated in the current stream if *Destination IPv4 address from* is set to *Manual*. The address is entered in decimal, four-dotted format. Any address between 0.0.0.0 and 255.255.255.255 is admitted as a destination IPv4 address.
Destination IPv4 address (DNS)	Destination IPv4 address carried by the packets generated in the current stream if *Destination IPv4 address from* is set to *Host name*. This is a read only field that it cannot be edited directly. It displays the result of the DNS name resolution carried out with the host name configured in *Destination host name.*
Destination host name	Domain name to be used as a destination if *Destination type* is set to *Domain name*. Unlike IP addresses, domain names are easy-to-remember alphanumeric strings but they have to be translated to IP addresses before any packet can be sent to the destination. The translation process requires the intervention of at least one DNS server. The DNS server IP address has to be configured in the local port profile either statically or by means DHCP.
Timeout	Time the receiver waits for an ICMP Echo replay for each ICMP Echo request it generates. No new Echo request is issued until either the previous reply is received or the timeout period finishes without any Echo reply reception. The default value for *Timeout* is 5.0 seconds.
Interval	Separation between two consecutive ICMP transmissions. The effective separation may be longer than the value configured in this field if the time it takes to receive the corresponding ICMP Echo reply is longer than the *Interval*. The default value for *Interval* is 1.0 seconds
ICMP packet size	Packet size used in transmitted ICMP Echo requests. In order to obtain the total frame size it is necessary to add the ICMP header length (8 bytes), IPv4 datagram header length (20 bytes) and the Ethernet (DIX) frame header and trailer (18 bytes). The default value is 56 bytes that is equivalent to a frame size of 102 bytes (56 bytes + 8 bytes + 20 bytes + 18 bytes).

Table 8.1: IP Ping Settings

Setting	Description
TTL	Initial *Time To Live* value configured in the packets transmitted in the current stream. The TTL is decreased by one unit each time it lefts a network node. If the value reaches zero, then the packet is discarded. The TTL is then a measure of the number of nodes the packet is allowed to transverse before reaching its destination.

8.1.3. Result verification

Ping results are presented in real time within a dedicated panel in the test unit. To display the Ping results follow these steps:

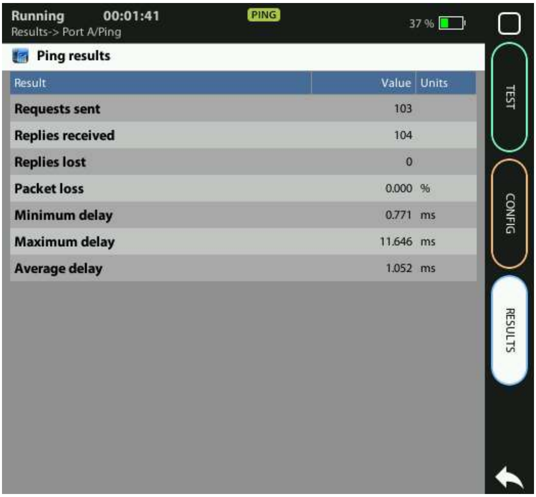
Table 8.2: IP Ping Results

Metric	Description
Requests sent	Number of ICMP Echo request messages sent from the beginning of the test.
Replies received	Number of ICMP Echo reply messages received from the destination. If the number of replies received is smaller than the request send, then it can be concluded than the network has dropped some packets. On the other hand, if the replies number is higher than the request count, then the network is probably duplicating packets somewhere.
Replies lost	Is the count of ICMP Echo reply messages lost from the beginning of the Ping test.
Packet loss	This metric is the ratio between the ICMP Echo request messages sent and the ICMP Echo reply messages lost.
Minimum delay	Minimum delay between the Echo request message transmission and the corresponding Echo reply reception event , computed over all the available Echo request / reply pairs. The Ping minimum delay can be considered an estimate of the minimum round trip delay between source and destination but the Ping delay may include ICMP protocol processing delays in intermediate router and in the destination.

Table 8.2: IP Ping Results

Metric	Description
Maximum delay	Maximum delay between the Echo request message transmission and the corresponding Echo reply reception event computed over all the available Echo request / reply pairs,. The maximum delay figure is subject to the same non-zero processing delay uncertainties than the *Minimum delay*.
Average delay	Mean delay between Echo request transmission and Echo reply reception events computed over all the available Echo request / reply pairs. The mean ping delay is subject to the same processing delay uncertainties than the *Minimum delay*.

1. From the *Home* panel, go to *RESULTS*,
   The test port results panel is displayed.
2. Select *Port A* to enter in the port specific results.
3. Select *Ping*.
4. Check the *Requests sent*, *Replies received*, *Replies lost*, *Packet loss*, *Minimum delay*, *Maximum delay* and *Average delay* statistics.



Running 00:01:41
Results-> Port A/Ping

Ping results

Result	Value	Units
Requests sent	103	
Replies received	104	
Replies lost	0	
Packet loss	0.000	%
Minimum delay	0.771	ms
Maximum delay	11.646	ms
Average delay	1.052	ms

Figure 8.1: Tempo Ping results panel.

8.2. Traceroute

Traceroute can be defined as an extended Ping test that traces intermediate network elements between the source and destination. These elements are identified by their IP addresses. For this reason, Traceroute is often used to check the path the packets follow when they are transmitted to the network.The test unit support two different implementations of the Traceroute application based on different probe packets:

- *ICMP Traceroute*: The test equipment uses ICMP Echo request messages with increasing TTL values to identify the nodes in the test path. Each node decreases the TTL value in one unit before forwarding the test packet. If the TTL reaches the value of 0, then the hop replies with an ICMP Time to live exceeded message to the transmission source.
- *UDP Traceroute*: It works in a similar way than the UDP Traceroute but in this case the probe packet is a regular UDP packet directed to an arbitrary port rather than an ICMP Echo request message.

It is important to notice that some network elements located in the Traceroute test part will never be detected by this test as in is required that these elements implement the IP protocol stack reply to be able to reply to the probe packets. Ethernet switches, broadband modes operating in bridged mode and media converters fall in this category.

8.2.1. Test Configuration

Connection setup is the same for Traceroute and Ping tests. Traceroute also shares the simple and quick setup procedure with the Ping test. To configure Traceroute follow these steps:

1. Make sure that the Port A of your tester is connected to the network. The physical layer must be up and working (See section 4.1.1).
2. From the *Home* panel, go to *CONFIG*
   The test port settings panel is displayed.
3. Configure *IP endpoint* with the help of the *Mode* setting.
4. Go to the *TEST* tab,
   The test configuration panel is displayed.
5. Configure *Ping/Traceroute* to *Traceroute*
6. Go to the *CONFIG* tab*,*
   The test port settings panel is displayed.
7. Configure *IP endpoint* with the help of the *Mode* setting.
8. Select either Port A to enter in the port specific configuration.
9. Configure the *Local profile* (See section 2.3) either by means the DHCP protocol or by hand.
10. Go to *Ping/Traceroute*
11. Enter the destination IPv4 address by using the *Destination IPv4 address from*, *Destination IPv4 address* and *Destination host name*.

12. Configure the *Timeout*, *Interval*, *Max. number of hops*, *Number of packets/hop*, *Traceroute protocol* and *UDP port* (UDP Traceroute only) parameters for the test.
13. Run the Traceroute test with the help of *Run*.

Table 8.3: Traceroute Settings

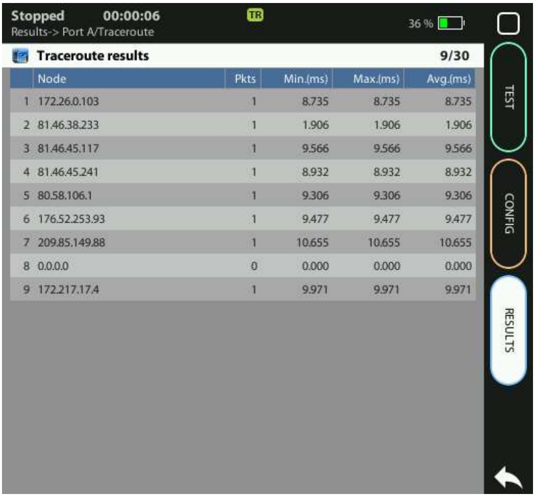
Setting	Description
Destination IPv4 address from	This field has the same meaning than the *Destination IPv4 address* from setting used by the Ping test (See section 8.1.2).
Destination IPv4 address	This field has the same meaning than the *Destination IPv4 address* setting used by the Ping test (See section 8.1.2).
Destination IPv4 address (DNS)	This field has the same meaning than the *Destination IPv4 address (DNS)* setting used by the Ping test (See section 8.1.2).
Destination host name	This field has the same meaning than the *Destination host name* setting used by the Ping test (See section 8.1.2).
Timeout	Time the receiver waits for an ICMP Time-to-live exceeded reply for each UDP request (UDP Traceroute) or ICMP Echo request (ICMP Traceroute). No new UDP / ICMP Echo request is issued until either the previous reply is received or the timeout period finishes without any Echo reply reception. The default value for *Timeout* is 5.0 seconds.
Interval	Separation between two consecutive ICMP / UDP transmissions. The effective separation may be longer than the value configured in this field if the time it takes to receive the corresponding ICMP Port unreachable / Time-to-live exceeded is longer than the *Interval*. The default value for *Interval* is 1.0 seconds
Max. Number of hops	Maximum length of the path to be analysed with Traceroute expressed in the number of hops (routers, hosts) it contains. The test fails to reach the end point if the path to be tested contains more hops than the number configured in this field. The default number of hops is 30.
Number of packets/ hop	Number of test packets directed to each hop in the test path. The default is 1 hop but this value could be increased to reduce the variability of delay statistics or to get more accurate packet loss statistics.

Table 8.3: Traceroute Settings

Setting	Description
Traceroute protocol	It is one of ICMP or UDP. These protocols define totally different Traceroute probe packets • ICMP: Uses ICMP Echo request messages with increasing TTL values as probe packets. • UDP: Uses UDP requests with increasing TTL values directed to a user configurable port as probe packets.
UDP port	Configures the destination UDP port used in UDP Traceroute tests. This setting is not required for ICMP Traceroute tests.

8.2.2. Result verification

Traceroute results are presented in real time within a dedicated panel in the test unit. To display the Traceroute results follow these steps:



Stopped 00:00:06
Results-> Port A/Traceroute

Traceroute results 9/30

	Node	Pkts	Min.(ms)	Max.(ms)	Avg.(ms)
1	172.26.0.103	1	8.735	8.735	8.735
2	81.46.38.233	1	1.906	1.906	1.906
3	81.46.45.117	1	9.566	9.566	9.566
4	81.46.45.241	1	8.932	8.932	8.932
5	80.58.106.1	1	9.306	9.306	9.306
6	176.52.253.93	1	9.477	9.477	9.477
7	209.85.149.88	1	10.655	10.655	10.655
8	0.0.0.0	0	0.000	0.000	0.000
9	172.217.17.4	1	9.971	9.971	9.971

Figure 8.2: Tempo Traceroute results panel.

1. From the *Home* panel, go to *RESULTS*,
   The test port results panel is displayed.
2. Select *Port A* to enter in the port specific results.
3. Select *Traceroute*.

4. Check the *Node* list and the *Pkts*, *Min.(ms)*, *Max.(ms)* and *Avg.(ms)* statistics for each node in the list.

Table 8.4: Traceroute Results

Result	Description
Node	IP address corresponding to a network node detected by the Traceroute test. The are displayed in a list following the same order than they have been detected by the probe packets.
Pkts	Number of ICMP Time to live exceeded messages received from a particular node in the path.
Min. (ms)	Minimum delay between the probe packet transmission and the corresponding ICMP reply reception event computed over all request / reply pairs for a particular node The Traceroute minimum delay can be considered an estimate of the minimum round trip delay between the source and the node but the Traceroute delay may include protocol processing delays in intermediate network elements.
Max. (ms)	Maximum delay between the probe packet transmission and the corresponding ICMP reply reception event computed over all request / reply pairs for a particular node. The maximum delay figure is subject to the same non-zero processing delay uncertainties than the *Min. (ms)* delay
Avg. (ms)	Maximum delay between the probe packet transmission and the corresponding ICMP reply reception event computed over all request / reply pairs for a particular node. The mean ping delay is subject to the same processing delay uncertainties than the *Min. (ms)* delay*.*

Chapter 9
PTP and NTP Analysis

Tempo may optionally supply *Packet Time Protocol (PTP)* and *Network Time Protocol* (NTP), emulation and analysis features.Some of the potential applications for the PTP / NTP emulation and testing capabilities included in Tempo are:

- PTP grandmaster or NTP server emulation synchronized with an external clock source based on GNSS, 1544 kHz, 2048 kHz, 1 PPS, ToD, IRIG-B, Synchronous Ethernet and other interfaces.
- PTP slave / NTP client emulation with extended performance measurements from the associated grandmaster and network, including master identity and status, PDV analysis and frequency / phase offsets.
- PTP / NTP pseudo-slave / pseudo-client operation. In this mode the test unit behaves in the same way than any standard PTP slave but indeed does not get synchronization from any PTP grandmaster / NTP server but from a clock reference chosen by the user. This test enables evaluation of metrics to quantify slow phase perturbations in the PTP timing such as TE, MTIE and TDEV. The Floor delay population test is also to be run in this operation mode.
- Passive monitoring testing of the communication between PTP entities. Connection of the passive monitor could be done in end-point or pass-through modes. Supported monitoring tests are related with master identity and status, PDV analysis and frequency offset.

9.1. Ethernet Synchronization with PTP and NTP

The *Network Time Protocol* (NTP), is one of the oldest protocols still in use and it is available in two flavours: the full version and Simple NTP (SNTP), a subset of NTP. On the other hand, the Precision Time Protocol (PTP), included in IEEE standard 1588 was originally designed to provide timing for critical industrial automation. With the 2008 version of this standard (IEEE 1588v2), PTP overcomes effects of latency and jitter through chains of Ethernet switches, providing accuracy in the nanosecond range.

9.1.1. NTP Synchronization

The latest version of NTP, version 4 (NTPv4) can usually maintain time to within 1- 20 ms using traditional software-interrupt based solutions over the public Internet and can achieve accuracies of microseconds or better in LANs under ideal conditions. NTP has been the most common and arguably the most popular synchronization solution, because it performs well over LANs and WANs and at the same time it is inexpensive, requiring very little hardware.

NTP should be able to deliver accuracy in the microsecond range on a controlled LAN and 1-20 ms on a WAN. However, protocol performance is far from guaranteed largely because of variable delays added by switches and routers.

9.1.2. PTP Protocol Details

PTP requires a central grandmaster clock and low-cost PTP slave clock sites. Master and slave network devices are kept synchronized by the transmission of timestamps transmitted within the PTP messages.

Depending on how many ports has a network clock, it is referred by the IEEE 1588 standard as an *Ordinary Clock* (single port device) or a *Boundary Clock* (multi port device). The version 2 standard also defines the concept of *Transparent Clocks* that improve timing accuracy when the protocol is run in network paths which contain intermediate switches.

Table 9.1: IEEE 1588v2 Device Description

Device	Description
Ordinary Clock	A single port device that can be a master or slave clock.
Boundary Clock	A multi port device that can be a master or slave clock.
End-to-end Transparent Clock	A multi port device that is not a master or slave clock but a bridge between the two. Forwards and corrects all PTP messages.
Peer-to-peer Transparent Clock	A multi port device that is not a master or slave clock but a bridge between the two. Forwards and corrects Sync and Follow-up messages only.
Management Node	A device that configures and monitors clocks.

The normal execution of the PTP has two phases:

1. *Master-Slave hierarchy establishment*. Ordinary and boundary clocks decide which port has the master or slave role in each link with the help of the Best Master Clock (BMC) algorithm. The information required for operation of the BMC is supplied by special *Announce* messages generated periodically by Ordinary and Boundary Clocks.

2. *Clock synchronization*. Slave clocks may have a positive or negative offsets when compared with their masters and latency from masters to slaves is also unknown. PTP devices start a procedure to compute latencies and offsets. These parameters will be used to adjust timing in slave devices.

9.1.3. PTP Synchronization Mechanism

Once the master and slave hierarchies have been established, by observing the clock property information contained in *Announce* messages sent by PTP devices, the synchronization process starts.

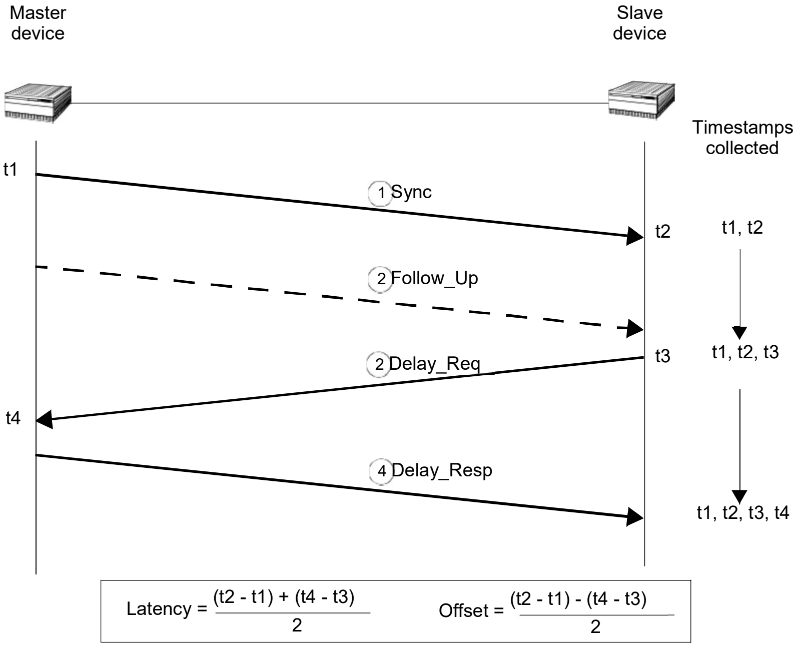


Figure 9.1: Sync and Delay request-response mechanisms used by the PTP. The basic parameters of Latency and Offset are computed from the t1, t2, t3 and t4 timestamps.

Before synchronization between the master and the slave clock has been achieved, it may exist a frequency offset between both clocks. This offset is computed with the help of the *Sync* message. *Sync* messages are sent periodically by the master to upgrade offset information in the slave. *Sync* messages may carry an accurate times-tamp indicating the departure time of the own message but this requires timestamping hardware which may not always be available. To avoid dedicated hardware *Follow_Up* messages can be used. *Follow_Up* messages carry timestamps for a previous *Sync* message allowing a more relaxed timestamping procedure and simpler hardware.

The *Sync* mechanism, however, does not take into account propagation time of *Sync* messages through the network. For this reason, the slave may request a latency measurement with a *Delay Req* message. Masters reply to a *Delay Req* with *Delay_Resp* message. The timestamps the slave gets from the Delay Request-Response mechanism are used to achieve accurate time synchronization in the slave clock.

The most difficult challenge of PTP is operation through chains of Ethernet switches. Most switches store packets in local memory while the MAC address table is searched and the cyclic redundancy check field of the packet is verified before it is sent out on the appropriate port/s. This process introduces variations in the time latency of packet forwarding and damages accuracy of the PTP protocol. Version 1 of the PTP protocol deals with this problem by implementing Boundary Clocks within the switches. Version 2 uses the innovative concept of Transparent Clock to deal with the same problem.

Transparent clocks do not participate in the master-slave hierarchy but they process PTP messages by adding special correction fields within the message based on their own estimations of packet residence times in the device. There are two different kinds of Transparent Clocks depending on whether they use the Peer-delay mechanism or the Delay request-response mechanism to compute the propagation delay between master and slave. The Peer-delay mechanism is more sophisticated and it has more pre-requisites than the Delay-request response mechanism but the Peer-delay mechanism is more scalable. End-to-end Transparent clocks add residence time compensations to all the PTP event messages but Peer-to-peer Transparent Clocks are only required to compensate *Sync* and *Follow-up* messages because they do not use the *Delay_Req* and *Delay_Resp* (Delay request-response mechanism) and they do not need to forward the *Pdelay_Req* and *Pdelay_resp* messages (Peer delay mechanism).

9.1.4. PTP Protocol Encapsulation

PTP messages can be carried over a large family of protocols including IPv4, IPv6, IEEE 802.3 Ethernet, DeviceNET, ControlNET and IEC 61158 Type 10. The most important encapsulations are the IP and Ethernet variations (see Figure 9.2:).

IEEE 1588 messages encapsulated in Ethernet frames use the special 0x88f7 Ethertype, specifically reserved for this purpose. Messages associated with the peer-delay mechanism carry the 01:1B:19:00:00:00 multicast destination address while the remaining messages carry the 01:80:C2:00:00:0E multicast address. On the other hand, messages encapsulated in IPv4 datagrams, use the UDP protocol for transport and the destination port is 319 (event messages) or 320 (all other messages). Multicast addresses to be used when the encapsulation is set to IPv4 are the 224.0.0.107 (peer delay mechanism messages) and the 224.0.1.129 (all other messages).

9.1.5. Unicast Addressing Mode

The IEEE 1588v2 standard also allows for a unicast communication architecture different to the multicast operation. Unicast is to be used in networks with no support

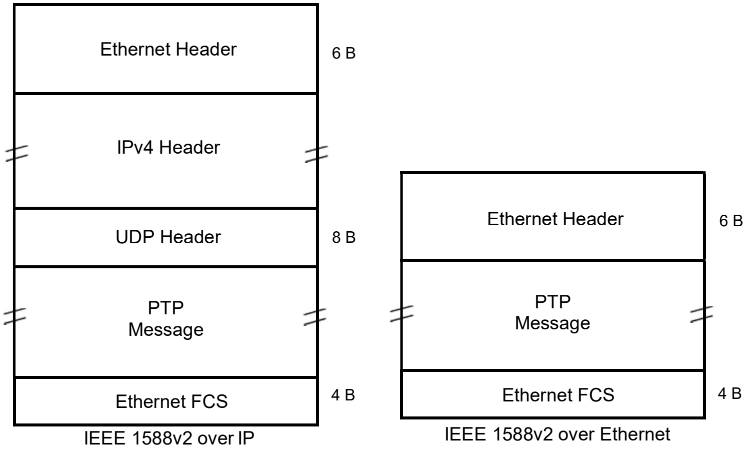


Figure 9.2: IP and Ethernet encapsulations for PTP messages.

of multicast mechanisms such as most of the current implementation of the Internet. In fact, unicast addressing has been adopted by ITU-T G.8265.1 that defines a PTP profile for frequency synchronization through IP networks. The ITU-T G.8265.1 profile applies to the UDP encapsulation only. It adopts the Signalling message format defined in IEEE 1588v2 to exchange information between PTP endpoints. The ITU-T G.8265.1 also defines some complementary mechanisms to ensure the interoperability of entities implementing this PTP profile.

Without an special configuration, unicast endpoints are unable to exchange any PTP message because they don't know the identity of the remaining endpoints. Operation in unicast mode therefore requires the configuration of suitable remote PTP entities (by means their IP address) in at least some devices. This is usually done in the devices willing to become slaves. These devices then initiate a dialogue with the grandmaster to negotiate the exchange of different PTP message types including *Announce*, *Sync* and *Delay reply*. Only when the delivery of these messages is granted by the grandmaster the synchronization process starts.

9.2. IEEE 1588 Grandmaster and Slave Emulation

Tempo can be configured to behave as different kinds of PTP entities, including PTP master and slave clocks. Theoretically, there is no difference between any standard PTP clock and these equipments but the testers supply measurement results that are useful to qualify the stability of a PTP timing source, the network performance when delivering different IEEE 1588v2 messages and the ability of PTP slaves to recover an accurate timing from the messages they receive from their masters:

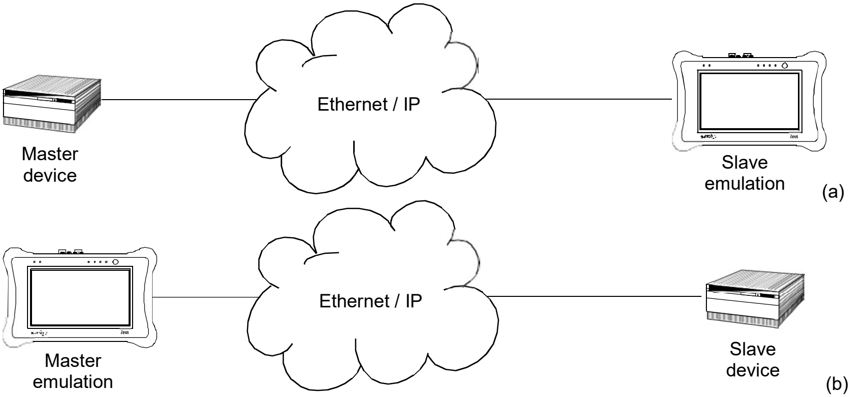


Figure 9.3: IEEE 1588 master and slave emulation modes: (a) Connection diagram corresponding to the PTP slave emulation mode, (b) connection corresponding to the master emulation mode.

The IEEE 1588 test results provided by Tempo when they are configured in *Clock emulation* mode can be classified in four different families:

- *Protocol state*: Not specifically test results. The protocol state contains details received from the master or the grandmaster clock (or the own test equipment when configured in master emulation mode).
- *Message statistics*: Includes message counts classified by their type (*Sync*, *Delay Request*, *Follow up*,...).
- *Delay statistics*: The *Packet Delay Variation* (PDV) and the *Packet Total Delay* (PTD) are some of the test results included in this family. Among different things, the delay statistics are useful to measure fast variations in the network transmission conditions affecting the timing accuracy of PTP slave devices.
- *Slave clock status*. When the test unit is configured in slave emulation mode, it tracks the frequency and phase of a PTP master. Due to phase / frequency instability in the master clock, or impairments caused by transmission through the packet switched network, the slave clock has to continuously adjust its frequency and phase. This test result quantifies the difference between the local (slave) clock and the estimated frequency / phase received from the master.

The exact test results available in any case depend on the current operation mode and on the test port. Port B contains a reduced set of PTP test results (*message statistics*) and it is unable to generate any message on its own. For this reason, for a full PTP analysis in master or slave emulation mode, it is recommended to connect the equipment to the network through the port A. Details about which results are available in each mode are provided in the following sections.

9.2.1. Configuration of the PTP Master and Slave

When configuring the test unit in master or slave emulation modes, it has to be taken into account that only the test Port A contains a full implementation of the protocol. Port B can be used to collect message statistics but transmission and decoding of PTP messages required to supply synchronization to remote entities (master emulation mode) or to synchronize the own clock with a remote entity (slave mode) are available for Port A only.

The IEEE 1588 slave and master clock emulation is compatible with the *Ethernet endpoint* and *IP endpoint* operation modes (See section 2.1). Configuration is slightly different in each case. If you are operating in *IP endpoint* mode you need to configure your local profile before you can run a PTP test. To do that, the required steps are:

1. From the *Home* panel, go to *CONFIG*
   The test port settings panel is displayed.
2. Select *Port A* to enter in the port specific configuration.
3. Configure the *Local profile* (See section 2.3) either by means the DHCP protocol or by hand.

The previous steps are not required if the equipment is operating in *Ethernet endpoint* mode. To run a PTP test (either in *Ethernet endpoint* mode or *IP endpoint* modes) follow these steps:

1. From the *Home* panel, go to *TEST*,
   The test configuration panel is displayed.
2. Go to *PTP (IEEE 1588)*.
3. Configure the equipment to become an active IEEE 1588 entity by configuring *PTP test* to *Emulation*.
   A label with the text PTP is displayed in the top notification area.
4. Configure *Clock emulation*, to *Master*, *Slave* or *Auto*, depending on your preferences.
5. Set the transport protocol to either *Ethernet* or *UDP*.
   Note: If you are operating in *Ethernet endpoint* mode, the *UDP* transport protocol is not allowed.
6. Configure the *Addressing mode* to *Unicast*, *Multicast* or *Hybrid*, depending on the system where the test unit is to be connected.
7. Depending on the PTP profile implemented in your system, configure *Path delay mechanism* to either *End-to-end* or *Peer-to-peer*.
8. Configure the *Domain* to the right value for your network.
9. Configure the *Priority 1*and *Priority 2* fields to the right values. These values determine the PTP role (master or slave) to be played by the test unit when *Clock emulation* parameter is set to *Auto*.

10. If you have configured *Clock emulation* to *Master* or *Auto* configure the *Master* clock type to *One-step* or *Two step* and set the *Clock class* and *Custom clock class* attributes.
11. If you have configured *Addressing mode* to *Unicast*, then you can configure one or more PTP entities to communicate with from the *Unicast master table* menu *Note*: Remote PTP entities are configured through their IP or MAC address, depending on the *Transport protocol.*
12. Configure the timing of the different messages associated to PTP from the *Message timing* menu
13. Optionally, configure the *Time properties* to custom values by setting the Mode field within this menu to Manual.

It must be taken into account that when the equipment is configured in slave emulation mode the timing is derived from the PTP messages it receives from the test interface. Any external reference such as GNSS or 1 PPS is ignored and could bedisabled. When the unit is configured to run in master emulation mode the time to be distributed is obtained from the external reference if the time is available (GNSS, ToD). With phase references (1 PPS) the PTP phase is still aligned with the reference but only the local system time could be distributed. With frequency references (2048 kHz, 2048 kb/s, 1544 kHz, 1544 kb/s, 10 MHz) both the phase alignment and the time are internally generated from the system clock but the PTP signal is still syntonized with the reference frequency.

Table 9.2: IEEE 1588 Settings

Setting	Description
PTP mode	Configures the IEEE 1588 test to be executed. These are the options currently available for this setting: • *None*: Disables all PTP generation and analysis. • *Emulation*: Choose this mode if you want the test unit to behave as a PTP slave or master clock. The unit becomes a new PTP entity in your network it will generate and receive IEEE 1588 messages in the same way than any other master / slave clock installed in your network once it is properly configured. • *Test*: Configures the unit as a PTP pseudo-slave that behaves in the same way than any standard PTP slave but doesn’t get synchronization from the IEEE 1588v2 grandmaster but from a clock reference chosen by the user. This is the correct operation mode to run a PTP *TE/ MTIE / TDEV* test or a *Floor Delay Population* test. • *Passive monitor*: This is the right mode to verify PTP communications between a PTP master and slave withoutdisturbing the transmission channel and the PTP entities.

Table 9.2: IEEE 1588 Settings

Setting	Description
Clock emulation	This setting enables the user to configure the role of the test unit within the PTP network. It is one of the following: • *Master*: The equipment is forced to assume the role of a PTP master clock within the network. • *Slave*: The equipment is forced to assume the role of a PTP slave clock within the network. • *Auto*: The equipment behaves as a PTP ordinary clock. It becomes a master or slave depending on the result of the BMC algorithm.
Transport Protocol	Configures the encapsulation protocol for the PTP messages. It is one of the following: • *Ethernet*: PTP messages are transmitted and received through an IEEE 802.3 / Ethernet encapsulation as specified in IEEE 1588-2008 Annex F. This transport protocol is used by the PTP Power profile (IEEE C37.238-2011) and the ITU-T G.8275.1 Telecom phase and time profile. • *UDP*: PTP messages are encapsulated in UDP over IPv4 frames as specified by IEEE 1588-2008 Annex D. This frame structure is used by the PTP Telecom profile for frequency synchronization (ITU-T G.8265.1) and the PTP Telecom profile for phase and time applications with partial timing support from the network (ITU-T G.8275.2).
Addressing mode	Defines the addressing procedure used by PTP endpoints to reach remote devices. It could be based in either multicast or unicast addressing: • *Unicast*: Enables unicast transmission of all PTP messages. For unicast addressing to work it is required knowledge from the endpoints about the remote end unicast address. Grandmasters know to which address to send messages thanks to a slave initiated handshake procedure based on time-limited leases but, if unicast operation is enabled, at least one grandmaster unicast MAC or IP address has to be configured in the slave. In the test unit grandmaster addresses are configured in the *Unicast master table*. Unicast addressing is used by the PTP Telecom profile for frequency synchronization (ITU-T G.8265.1) and the PTP Telecom profile for phase and time applications with partial timing support from the network (ITU-T G.8275.2).

Table 9.2: IEEE 1588 Settings

Setting	Description
Addressing mode	• *Multicast*: Configures multicast transmission in the PTP interface. It means that destination addresses of PTP messages transmitted by the interface will be multicast. If the current payload setting is UDP, then the correct destination addresses are 224.0.1.129 and 224.0.0.107. In Ethernet payloads the multicast addresses are 01:80:C2:00:00:0E and 01:1B:19:00:00:00. Multicast addressing is required by the PTP Power profile (IEEE C.37.238-2011) and the ITU-T G.8275.1 Telecom phase and time profile. • *Hybrid*: Some PTP messages are multicast and some other are transmitted in unicast mode. For unicast messages, the multicast addresses and standard lease mechanism is reused from the full multicast and unicast modes. In hybrid mode *Announce*, *Follow-up* and *Sync* messages are still generated in multicast mode but *Delay Request*, *Peer Delay Request* and *Peer Delay Follow-up* are transmitted as unicast messages.
Path delay mechanism	Decides whether to use the end-to-end or the peer-to-peer delay mechanism to compensate the latency between PTP endpoints. The available configurations are: • *End-to-end*: Delay is computed by exchanging delay request and reply messages between endpoints. This operation mode is used by the PTP Telecom profile for frequency synchronization (ITU-T G.8265.1),the ITU-T Telecom phase and time profile with full timing support from the network (ITU-T G.8275.1)and partial timing support from the network (ITU-T G.8275.2). • *Peer-to-peer:* Delay is computed by exchanging peer-delay request and reply messages between PTP peers. A PTP peer is not necessarily an endpoint. Intermediate devices such as transparent clocks may also participate in the peer delay mechanism. The PTP Power profile (IEEE C37.238-2011) is based in the peer-to-peer delay mechanism.

Table 9.2: IEEE 1588 Settings

Setting	Description
Master clock type	Configures generation of follow up packets for *Sync* and other PTP messages. This setting could have two different values: • *One-step:* Means that no follow up messages are generated. The time stamps are carried by *Sync* and *Peer Delay Response* messages themselves. • *Two-step*: In this case a follow up message is generated for each Sync and Peer Delay Response message. The Sync and Peer Delay Response messages provide information about meaningful transmission instants and the follow-ups are the time-stamps for these instants. No one of the methods is more accurate than the other but one-step clocks are more efficient because they generate less messages to send the same information. PTP slave clocks are required to be compatible with the one-step and two-step mechanisms. End-to-end slave clocks are required to accept follow up messages when received but they do not generate these messages themselves. Peer-to-peer messages on the other hand have to reply to peer delay requests from other PTP entities and therefore the clock type has to be configured in these clocks even if they do not operate as PTP masters.
Message timing	This menu contains menu items necessary to configure the timing associated to the transmission of several message types when the equipment is configured in clock emulation or test modes. With the help of the *Message timing* menu you can configure the following parameters: *Sync TX interval*, *Delay Request TX interval*, *Peer Delay Request TX interval*, *Announce TX interval*, *Announce RX timeout (#msgs)*, *Unicast Sync interval, Unicast Delay Request interval*, *Unicast Peer Delay Req. interval.*
Domain	Configures the PTP domain for the test unit. The PTP domain is identified by a number between 0 and 255. The equipment is allowed to exchange PTP information only with clocks within the same domain. The unit ignores all messages received from other domains (these messages are classified as *Domain mismatches*). All PTP equipments from other domains will probably ignore all messages from the tester.

Table 9.2: IEEE 1588 Settings

Setting	Description
Priority 1	This is a numeric parameter used by the BMC to establish the master / slave hierarchy with the help of the BMC algorithm. The range of accepted values of *Priority 1* is between 0 and 255. It is more likely that the test unit becomes a PTP master during the BMC if *Priority 1* is configured to an small value.
Priority 2	This is a numeric parameter used by the BMC to establish the master / slave hierarchy with the help of the BMC algorithm. The range of accepted values of *Priority 2* is between 0 and 255. It is more likely that the test unit becomes a PTP master during the BMC if *Priority 2* is configured to an small value.
Unicast master table	Contains a table where the user can configure one or several PTP peer addresses. By default, unicast entities do not receive any announcement message from other PTP devices deployed in the network. Before unicast clocks can exchange any piece of information with other PTP entity they need to establish an association with this entity. This is usually done with a slave initiated dialogue. In order to be able to start this dialogue, the unicast endpoint must know the IP addresses (UDP payload) or MAC addresses (Ethernet payload) corresponding with the peers. These are the addresses to be configured in this table. This configuration is required only when the unit is expected to operate as an slave. Multicast communications do not require setting of this table neither.
Unicast peer IPv4 address	The Unicast peer IPv4 address is the peer address configured when *Transport protocol* is *UDP*, *Addressing mode* is *Unicast* and the *Path Delay Mechanism* is configured to *Peer-to-peer*. When the peer-to-peer delay mechanism is configured in *Path delay mechanism*, message delivery happens between contiguous devices and it is not necessarily end-to-end. It is therefore required to configure the peer address which it is normally different to the remote end address.

Table 9.2: IEEE 1588 Settings

Setting	Description
Unicast peer MAC address	The Unicast peer IPv4 address is the peer address configured when *Transport protocol* is *Ethernet*, *Addressing mode* is *Unicast* and the *Path Delay Mechanism* is configured to *Peer-to-peer*. When the peer-to-peer delay mechanism is configured in *Path delay mechanism*, message delivery happens between contiguous devices and it is not necessarily end-to-end. It is therefore required to configure the peer address which is normally different to the remote end address.
Master identity	Menu that contains the menu items necessary to set the master identity either as a MAC address, IPv4 address or host name. You can also allow the equipment choose the master identity for you if you set the *Source of identity* subfield to *Auto*. Configuring the master identity makes sense only you have configured the equipment as a *Passive monitor*.
Clock class	Sets the clock class as defined in IEEE 1588-2008 orthe clock-source quality-level defined in ITU-T G.781. The Clock class defines traceability of the time or frequency distributed by the master clock and it is one of the parameters used to establish the master / slave hierarchy with the help of the BMC. This field is available for configuration only if *Clock emulation* has been set to *Auto* or *Master*.
Custom clock class	The *Custom clock class* sets a custom clock class in numeric format when *Clock class* has been configured to *Custom*. Any *Custom clock class* between 0 and 255 is allowed here.
Time Properties	Configures the values of certain flags related with traceability of the time and / or frequency signal generated by the test equipment when it is configured in PTP master emulation mode.
Clock id.	Read only field that reports the Clock Id. assigned to the PTP engine running in the port. The Clock Id. is built from the port A MAC address following IEEE 1588v2.
Port	Port number. In a multi-port PTP device with it identifies each port. Tempo have all one single PTP port andthere- fore the port number is always 1.

When the test unit is configured in endpoint mode and PTP entity emulation is enabled, the equipment can still be configured as a multistream traffic generator (See section 4.1, See section 4.2). This feature is useful to verify the performance of the PTP protocol with different traffic loads.

Table 9.3: IEEE 1588v2 Time Properties Settings

Setting	Description
Mode	It is one of *Manual* or *Auto* • *Manual*: The user decides the value of the time properties fields and flags. This setting is required if detailed debug of the PTP master-to-slave association is required. For example some slaves may refuse get locked to the master when the time or frequency is not traceable. • *Auto*: Lets the test unit decide which settings to use for the time properties. The equipment always tries to use the best time source available. For example, it uses TAI time scale if possible and it sets the correct UTC offset if this information is available. Specifically, when either a phase or a frequency reference is used the automatic time scale is always *Arbitrary*.When a time reference (GNSS, ToD) is used the time scale is TAI but a transient Arbitrary time scale could be transmitted for a few minutes before the GNSS receiver has got from the satellite system all the information required to generate an accurate TAI time. Using *Manual* time properties does not make sense if the unit is not operating in PTP master emulation mode. For this reason, this control is configured statically to *Auto* in slave emulation mode.
UTC Offset	This field reports the difference between the TAI and UTC time scales. Due to the leap seconds mechanism this offset is always an integer number of seconds. Currently (February 2019), the TAI time is 37 seconds ahead of UTC. The UTC offset is required only if the slave has to translate the time into the UTC time scale. All Tempo time measurements in test mode are done in the TAI time scale and therefore they are not affected by the value of this flag
UTC Offset valid	The value of this flag is true if the value configured in the UTC offset is usable by slave (or boundary) clocks.

Table 9.3: IEEE 1588v2 Time Properties Settings

Setting	Description
Timescale	The time scale is an standard for the duration of the time unit (usually the atomic second) together with an epoch, which constitutes an origin for the seconds count. It is one of *Arbitrary* or *TAI.* - *Arbitrary:* It means that a custom time scale is being distributed. Basically, any non-TAI time scale, included UTC, is considered arbitrary. In an arbitrary time scale there is no control on the second length or in the epoch time. There is also the possibility of unexpected gaps in seconds count. - *TAI*: International Atomic Time. Weighted average of the time kept by about 200 atomic clocks in over 50 national laboratories worldwide. It is a continuous time scale (it contains no leap seconds), it uses the atomic second as a time unit. The epoch for the TAI time scaleis 00:00:00 01/01/1970.
Time traceable	This flag is set to true when the time provided by a network clock is traceable to a primary time source. For example, the GPS satellite constellation is time traceable.
Frequency traceable	This flag is set to true when the time provided by a network clock is traceable to a primary frequency source. Forexample, the GPS satellite constellation is frequencytraceable.
Time source	Sets the time source used by the grandmaster clock in a certain PTP domain. It could be one of: *Atomic clock*, *GPS*, *Terrestrial radio*, *PTP*, *NTP*, *Hand-set*, *Internal oscillator*, *Others.*

In any PTP endpoint emulation test it is important to pay attention to the PTP message timing. There is a menu specifically devoted to configure the timing for the different PTP messages (*Message Timing* menu). As an example, configuring the correct *Announce TX interval* and *Announce TX timeout (#msgs)* is essential even if the unit is going to play the slave role. This is because the test unit may wrongly understand that one or several messages are lost and trigger the actions corresponding to this event.

Table 9.4: IEEE 1588v2 Message Timing Configuration

Setting	Description
Sync TX interval	Sync message rate transmitted by the test unit when the *Addressing Mode* is configured to *Multicast*. Allowed values are 128 pkt/s, 64 pkt/s, 32 pkt/s, 16 pkt/s, 8 pkt/s, 4 pkt/s, 2 pkt/s, 1 pkt/s, 2 s/pkt, 4 s/pkt and 8 s/pkt. Sync messages are not transmitted by PTP slaves and therefore this setting is enabled only if *Clock emulation* is set to *Auto* or *Master*.
Delay Request TX interval	Delay Request message rate transmitted by the test unit when the *Addressing Mode* is configured to *Multicast*. Allowed values are 128 pkt/s, 64 pkt/s, 32 pkt/s, 16 pkt/s, 8 pkt/s, 4 pkt/s, 2 pkt/s, 1 pkt/s, 2 s/pkt, 4 s/pkt and 8 s/pkt. Delay Request messages are not transmitted by PTP grandmasters and therefore this setting is enabled only if *Clock emulation* is set to *Auto* or *Slave*. If the *Path delay mechanism* is configured to *Peer-to-peer* then Peer Delay Request rather than Delay Request messages are transmitted and therefore this field is greyed out.
Peer Delay Request TX interval	Peer Delay Request message rate transmitted by the test unit when the *Addressing Mode* is configured to *Multicast*. Allowed values are 128 pkt/s, 64 pkt/s, 32 pkt/s, 16 pkt/s, 8 pkt/s, 4 pkt/s, 2 pkt/s, 1 pkt/s, 2 s/pkt, 4 s/pkt and 8 s/pkt. Peer Delay Request messages are not transmitted by PTP grandmasters and therefore this setting is enabled only if *Clock emulation* is set to *Auto* or *Slave*. The *Path delay mechanism* must be also configured to *Peer-to-peer* to enable these messages to be transmitted.
Announce TX interval	Configures the Announce message rate. It is important that this parameter is homogeneous in all PTP entities in the domain. Allowed values for the Announce TX interval are 8 pkt/s, 4 pkt/s, 2 pkt/s, 1 pkt/s, 2 s/pkt, 4 s/pkt, 8 s/pkt, 16 s/pkt, 32 s/pkt, 64 s/pkt, 128 s/pkt and 256 s/pkt.

Table 9.4: IEEE 1588v2 Message Timing Configuration

Setting	Description
Announce RX timeouts (#msgs)	Sets the number of missing Announce packets before a PTP slave declares the timing source to be lost. Any value between 2 and 10 messages is allowed. Only PTP slaves are expected to keep track of received Announce messages and therefore, this option is greyed out if *Clock emulation* is configured to *Master*.
Unicast Sync interval	Sync message rate negotiated by unicast PTP entities. If the entity finally becomes a grandmaster it will deliver packets at the negotiated rate. Both grandmasters and slaves participate in the unicast Sync interval negotiation and therefore, unlike it happens in the multicast addressing mode, this setting makes sense in all clock emulation modes. Allowed values for the *Unicast Sync interval* are 128 pkt/s, 64 pkt/s, 32 pkt/s, 16 pkt/s, 8 pkt/s, 4 pkt/s, 2 pkt/s, 1 pkt/s and 2 s/pkt.
Unicast Delay Request interval	Delay requestmessage rate negotiated by unicast PTP entities. If the entity finally becomes an slave it will deliverpackets at the negotiated rate. Both grandmasters and slaves participate in the unicast Delay Request interval negotiation and therefore, unlike it happens in the multicast addressing mode, this setting makes sense in all clock emulation modes. If the *Path delay mechanism* is configured to *Peer-to-peer* then Peer Delay Request rather than Delay Request messages are transmitted and therefore this field isgreyed out. Allowed values for the *Unicast Delay Request interval* are 128 pkt/s, 64 pkt/s,32 pkt/s, 16 pkt/s, 8 pkt/s, 4 pkt/s, 2 pkt/s, 1 pkt/s, 2 s/pkt, 4 pkt/s, 8 pkt/s, 16 pkt/s, 32 pkt/s, 64 pkt/s.

Table 9.4: IEEE 1588v2 Message Timing Configuration

Setting	Description
Unicast Peer Delay Req. interval	Peer Delay Request message rate negotiated byunicast PTP entities. If the entity finally becomes an slave itwill deliver packets at the negotiated rate. Both grandmasters and slaves participate in the unicast Peer Delay Request interval negotiation and therefore, unlike it happens in the multicast addressing mode, this setting makes sense in all clock emulation modes. The *Path delay mechanism* must also configured to *Peer-to-peer* to enable these messages to be transmitted. Otherwise, Delay Request rather than Peer Delay Request messages will be transmitted. Allowed values for the *Unicast Peer Delay Request interval* are 128 pkt/s, 64 pkt/s, 32 pkt/s, 16 pkt/s, 8 pkt/s, 4 pkt/s, 2 pkt/s, 1 pkt/s, 2 s/pkt, 4 pkt/s, 8 pkt/s, 16 pkt/s, 32 pkt/s, 64 pkt/s.

9.2.2. Protocol State

The basic PTP results are available in the *Protocol State* panel. All the information contained in this panel is collected from *Announce* messages received from remote PTP entities or is an indication of the state of the internal PTP synchronization machine.

The *Protocol State* results are permanent, it is not required to start a test (*RUN* button) to display the information from this panel. The information is updated in real-time as new changes in the protocol state are registered by the test unit. To display the protocol state panel follow these steps:

1. From the *Home* panel, go to *RESULTS*,
   The test port results panel is displayed.

2. Select either *Port A* to enter in the port A specificresults.

Table 9.5: Protocol State Results

Result	Description
Port state	Displays one of the port states defined for the BMC algorithm in standard IEEE 1588-2008. These states determine which is the current role of the network equipment within the synchronization network (master or slave) or inform about special conditions or problems within the BMC algorithm. The Port State is set to one of the following values: • *Initializing*: While a port is in the *Initializing* state, the port initializes its data sets, hardware, and communication facilities. The port does not place any PTP messages on its communication path. • *Faulty*: The fault state of the protocol. A port in this state does not place any PTP messages. • *Disabled*: The port does not place any messages onits communication path. All PTP received messages are ignored except for statistic compilation. • *Listening*: The port is waiting for an announce receipt timeout to expire or to receive an *Announce* message from a master. The purpose of this state is to allow orderly addition of clocks to a domain. • *Pre-master*: The port behaves in all respects as though it were in the *Master* state except that it does not placeany messages on its communication path except for *Peer Delay Request*, *Peer Delay Response* or *Peer Delay Follow up*. • *Master*: The port is behaving as a master clock. • *Passive*: The port does not place any messages on its communication path except for *Peer Delay Request*, *Peer Delay Response* or *Peer Delay Follow up*. • *Uncalibrated*: One or more master ports have been detected in the domain. The appropriate master port has been selected, and the local port is preparing to synchronize to the selected master port. This is a transient state to allow initialization of synchronization servos, updating of data sets when a new master port has been selected. • *Slave*: The port is synchronizing to the selectedmaster port.

Table 9.5: Protocol State Results

Result	Description
Master IP address	This is a 32-bit IPv4 address in the standard four-dotted decimal format *A.B.C.D* that describes the master. This result is displayed only if the PTP *Transport Protocol* is - *UDP*. If the test equipment is operating in master emulation mode or if there is no master, the IP address corresponding to the active PTP port in the unit is shown instead.
Master Ethernet address	48-bit MAC address in the standard hexadecimal-digit format *XX:XX:XX:XX:XX:XX* corresponding to the PTP master where the test unit is currently connected. This result is displayed only if the PTP *Transport Protocol* is - *Ethernet*. If the test equipment is operating in master emulation mode or if there is no master, the MAC address corresponding to the active PTP port in the unit is shown instead.
Master identity	EUI-64 code associated to the master clock. The EUI-64, computed as explained in standard IEEE 1588-2008, constitutes a globally unique identifier.
Master port number	Number of ports reported by the master. Devices with one port are referred as Ordinary Clocks by IEEE 1588v2. Devices with more than one port are termed as Boundary Clocks.
Tiimescale	The time scale is an standard for the duration of the time unit (usually the atomic second) together with an epoch, which constitutes an origin for the seconds count. It is one of *Arbitrary* or *TAI.* • *Arbitrary:* It means that a custom time scale is being distributed. Basically, any non-TAI time scale, included UTC, is considered arbitrary. In an arbitrary time scale there is no control on the second length or in the epoch time. There is also the possibility of unexpected gaps in seconds count. • *TAI*: International Atomic Time. Weighted average of the time kept by about 200 atomic clocks in over 50 national laboratories worldwide. It is a continuous time scale (it contains no leap seconds), it uses the atomic second as a time unit. The epoch for the TAI time scale is 00:00:0001/01/1970.

Table 9.5: Protocol State Results

Result	Description
Grandmaster identity	EUI-64 code associated to the grandmaster clock. The EUI-64, computed as explained in standard IEEE 1588-2008, constitutes a globally unique identifier. The Grandmaster identity is different to the master identity only when the synchronization is transmitted through a chain involving several PTP master / slave relations.
Grandmaster priority 1	Priority 1 parameter configured in the grandmaster. The *priority 1* is a numeric parameter used by the BMC algorithm to establish the master / slave hierarchy. The smaller this value is, the higher priority is assigned to the clock to become master.
Grandmaster priority 2	Priority 2 parameter configured in the grandmaster. The *priority 2* is a numeric parameter used by the BMC algorithm to establish the master / slave hierarchy. The smaller this value is, the higher priority is assigned to the clock to become master.
Grandmaster clock class	Clock class associated to the grandmaster clock in decimal format. The Clock class defines traceability of the time or frequency distributed by the master clock and it is one of the parameters used to establish the master / slave hierarchy with the help of the BMC.
Grandmaster clock class desc.	Clock class associated to the grandmaster clock described with alphanumeric characters. Examples of possible clock class descriptors are: *Custom*, *Synchronized to PRC*, *Holdover*, *Default,* etc.
Grandmaster clock accuracy	The grandmaster clock accuracy indicates the expected accuracy of a clock when it is the grandmaster, or in the event it becomes the grandmaster. This is a field that characterized a clock for the purpose of determining the master / slave hierarchy.
Grandmaster clock variance	Grandmaster clock statistic variance estimated as specified in IEEE 1588-2008. This field is used by the grandmaster clock to report the variability of its own internal oscillator.

Table 9.5: Protocol State Results

Result	Description
Grandmaster time source	Indicates the time source used by the grandmaster clock. The value is not used in the selection of the grandmaster clock. It is one of the following • *Atomic clock*: Any device that is based on atomic resonance for frequency and that has been calibrated against international standards for frequency and time. • *GPS*: Any device synchronize to a satellite system that distribute time and frequency tied to international standards. • *Terrestrial radio*: Any device synchronized via any of the radio distribution systems that distribute time and frequency tied to international standards • *PTP*: Any device synchronized to a PTP-based source of time external to the domain • *NTP*: Any device synchronized via the Network Time Protocol (NTP) or the Simple Network Time Protocol (SNTP) to servers that distribute time and frequency tied to international standards. • *Hand set*: Used for any device whose time has been set by means of a human interface based on observation of an international standards source of time to within the claimed clock accuracy. • *Other*: Other source of time and / or frequency not covered by other values. • *Internal oscillator*: Any device whose frequency is not based on atomic resonance nor calibrated against international standards for frequency, and whose time is based on a free running oscillator with epoch determined in an arbitrary or unknown manner.

3. Enter in *PTP* to display results about the PTP protocol.
4. Go to *Protocol state* and check *Port state*, *Master IP address / Master Ethernet address*, *Master identity*, *Master port number*, *Timescale, Grandmaster identity*, *Grandmaster priority 1*, *Grandmaster priority 2*, *Grandmaster clock class*, *Grandmaster clock class desc.*,*Grandmaster clock accuracy*, *Grandmaster clock variance*, *Grandmaster time source*.

9.2.3. Message Statistics

The *Message statistics* panel include counts of each PTP message type defined in IEEE 1588-2008. This result panel includes statistics both about received and transmitted (internally generated) packets.

There is one Message statistics panel for each test port. In case, that protocol emulation or delay / jitter tests are not required, Port B can be used for message statistics compilation. The procedure to display the message statistics is as follows:

1. From the *Home* panel, go to *RESULTS*,
   The test port results panel is displayed.
2. Select either *Port A or Port B* to enter in the port specific results.
3. Enter in *PTP* to display results about the PTP protocol.
4. Go to *Message statistics*.
5. Press *Run* to start a new test and check the transmitted (TX) and received (RX) values of *Sync*, *Delay Request*, *Delay Response*, *Peer Delay Request*, *Peer Delay Response*, *Follow-up*, *Peer Delay*, *Follow-up*, *Announce*, *Signaling*, *Management* and *Domain mismatch*,

Table 9.6: IEEE 1588 Message Statistics

Result	Description
Sync	Accounts for the number of received (RX) and transmitted (TX) *Sync* messages. *Sync* messages are generated by PTP master clocks and carry information about their clock frequency and phase. To achieve accurate synchronization the PTP slave needs to complement the information obtained from the Sync messages either with the Delay request-response or the Peer delay mechanisms.
Delay Request	Number of received (RX) and transmitted (TX) *Delay Request* messages. The *Delay Request* message is part of the *Delay request-response* mechanism used to measure the two-way latency between master and slave. The *Delay Request* message is always generated by the PTP slave.
Delay Response	Number of received (RX) and transmitted (TX) *Delay Response* messages. The *Delay Response* message is part of the *Delay request-response* mechanism used to measure the two-way latency between master and slave. The *Delay Response* message is always generated by the PTP master as a reply to a *Delay request* received from a slave.

Table 9.6: IEEE 1588 Message Statistics

Result	Description
Peer Delay Request	Computed number of received (RX) and transmitted (TX) *Peer Delay Request* messages. The *Peer Delay Request* message is part of the *Peer Delay* mechanism used to measure the two-way latency between master and slave.
Peer Delay Response	Number of received (RX) and transmitted (TX) *Peer Delay Response* messages. The *Peer Delay Response* message is part of the *Peer Delay request-response* mechanism used to measure the two-way latency between master and slave. The *Peer Delay Response* message is always generated by the PTP entity as a reply to a *Peer Delay Request* received from the peer entity.
Follow-up	Number of received (RX) and transmitted (TX) *Follow-up* messages. *Follow up* packets are generated by some PTP masters when for some reason *Sync* messages cannot carry accurate timestamps. In this case the a *Follow up* message carrying the accurate timestamps is transmitted immediately after every *Sync* packet.
Peer Delay Follow-up	Number of received (RX) and transmitted (TX) *Peer Delay Follow-up* messages. *Peer Delay Follow-up* packets are generated by some PTP devices using the *Peer delay* mechanism masters when for some reason *Sync* messages cannot carry accurate timestamps. In this case the a *Follow up* message carrying the accurate timestamps is transmitted immediately after every *Sync* packet.
Announce	Number of received (RX) and transmitted (TX) *Announce* messages. Announce messages are generated by PTP ordinary and boundary clocks in order to establish or modify a master / slave hierarchy by means the *Best Master Clock* (BMC) algorithm.
Signaling	Number of received (RX) and transmitted (TX) *Signalling* messages. *Signaling* messages are generated by PTP entities to negotiate some optional features like unicast transmission.

Table 9.6: IEEE 1588 Message Statistics

Result	Description
Management	Number of received (RX) and transmitted (TX) *Management* messages. Management messages are used to connect the PTP entities to the management system and enable operation and maintenance of the synchronization network.
Domain mismatch	Total count of received IEEE 1588 messages no corresponding to the currently configured PTP domain.
Sync seq. anomaly	This is a counter increased in one unit foreach out-of-order received Sync message. An out-of-order message contains a sequence number different to the expected value.

9.2.4. Delay Statistics

The *Delay statistics* panel is probably one of the most important PTP results panel available in *PTP clock emulation* mode as it contains valuable quantitative information to assess the performance of the transmission network. Like it happens with most of the PTP results, the *Delay statistics* are available only for Port A.

Delay statistics do not depend on the operation mode (*IP endpoint* or *Ethernet endpoint*) but they do on the clock role. For example, in master emulation mode, *Sync* messages are ignored and therefore all metrics related with this message are not available. The PTP delay statistics are compensated with the help of the correction field included in PTP event messages. The objective of the delay compensation is to evaluate the transmission performance achieved with switches behaving as transparent clocks. It is important to note that if the equipment is configured in slave emulation mode, some delay statistics may not be accurate. The reason is that in this mode the time reference is generated based on received PTP messages, which are at the same time the objects to be evaluated. One of the most visible effects is that any steady state long term estimation of the path asymmetry is zero. An alternative to improve the accuracy of the delay statistics is to use an external time reference (GNSS) and configure *PTP mode* to *Test* (pseudo-slave).

The procedure to display the delay statistics associated to PTP messages is as follows:

Table 9.7: IEEE 1588 Delay Statistics

Result	Description
Sync PTD (current)	Last calculated value of the *Packet Total Delay* (PTD) experienced by IEEE 1588 *Sync* messages when they travel from the master to the test unit (with *end-to-end* delay mechanism) or from the peer entity to the slave (with *peer-to-peer* delay mechanism). The result is expressed inmicroseconds. The Sync *PTD (current)* metric is compensated in delay which means that corrections carried out by intermediate IEEE 1588 transparent clocks are taken into account to compute the end result. This result is available only if the equipment is operating in *Slave emulation* mode or in *Test* mode.
Sync PTD (minimum)	Minimum value of *Sync PTD (current)* registered from the beginning of the test. This result is available if the equipment is operating in slave emulation mode or in test mode.
Sync PTD (maximum)	Maximum value of *Sync PTD (current)* registered from the beginning of the test. This result is available if the equipment is operating in slave emulation mode or in test mode.
Sync PTD (average)	Mean value of the PTD computed over all *Sync*messages received from the beginning of the test and expressed in microseconds. This result is available if the equipment is operating in slave emulation mode or in test mode.
Sync PTD (std. dev.)	Standard deviation of the PTD computed over all *Sync*messages received from the beginning of the test. Note that even if it is an statistic corresponding to the PTD, the standard deviation is a quantity related with how the PTD varies over the collected samples. In fact, the *Sync PTD (std. dev.)* does not depend on the absolute delay from the master and it is computed in slave emulation, pseudo-slave emulation (*Test mode*) and passive monitoring modes.

Table 9.7: IEEE 1588 Delay Statistics

Result	Description
Sync PTD (range)	Difference between the *Sync PTD (maximum)* and *Sync PTD (minimum)*. This is an Sync PTD statistic but like it happens with the *Sync PTD (std. dev.)* it is more related with delay variation than with absolute delay. It could be that the *Sync PTD (range)* is known even if *Sync PTD (maximum)* and *Sync PTD (minimum)* are not. For this reason, the *Sync PTD (range)* statistic is computed in slave emulation, pseudo-slave emulation (*Test mode*) and passive monitoring modes.
Sync PDV (current)	Current value of t the *Packet Delay Variation* (PDV) computed as per RFC 3393 and RFC 1889. Delay variation is computed over consecutively transmitted packets. The instantaneous value is smoothed with the function defined in RFC 1889 before being displayed. The *Sync PDV (current)* is computed in slave emulation, pseudo-slave emulation (*Test mode*) and passive monitoring modes.
Sync PDV (maximum)	Maximum value of *Sync PDV (current)* registered from the beginning of the test. The *Sync PDV (maximum)* is computed in slave emulation, pseudo-slave emulation (*Test mode*) and passive monitoring modes.
Sync PDV (average)	Mean value of all the Sync PDV values computed from the beginning of the test. Each individual delay variation is evaluated as the absolute value of the PTD associated to a given frame minus the PTD associated to the frame transmitted next. All possible consecutive frame transmission events are taken into account for the calculation of this performance metric. The only exception to this rule is if one or both frames are lost. The *Sync PDV (average)* is computed in slave emulation, pseudo-slave emulation (*Test mode*) and passive monitoring modes.
Delay req. PTD (current)	Last calculated value of the PTD experienced by IEEE 1588 *Delay req.* messages (or *Peer delay req.* messages) when they travel from the test unit to the master (with *end-to-end* delay mechanism) or from the test unit to the peer entity (with *peer-to-peer* delay mechanism).

Table 9.7: IEEE 1588 Delay Statistics

Result	Description
Delay req. PTD (minimum)	Minimum value of *Delay req. PTD (current)* registered from the beginning of the test. The *Delay req. PDV (minimum)* is computed both in slave emulation and test modes.
Delay req. PTD (average)	Mean value of the PTD computed over all *Delay req.* messages transmitted from the beginning of the test.
Delay req. PTD (std. dev.)	Standard deviation of the PTD computed over all Delay request messages received from the beginning of the test. This metric is computed when the equipment is operating in IEEE 1588 slave clock emulation or in test mode.
Delay req. PTD (range)	Difference between *Delay req. PTD (maximum)* and *Delay req. PTD (minimum)*. This metric is computed only in slave emulation and test modes.
Two-way PTD (current)	This result is computed as the sum of the *Sync PTD (current)* and *Delay req. PTD (current).* It is an estimation of the time invested by a two-way IEEE 1588 packet transmission between the master and the slave. This metric is computed in slave emulation mode and in test mode
Two-way PTD (minimum)	This result is computed as the sum of the *Sync PTD (minimum)* and *Delay req. PTD (minimum).* It is an estimation of the minimum time invested by a two-way IEEE 1588 packet transmission between the master and the slave. This metric is computed in slave emulation mode and in test mode.
Two-way PTD (average)	Metric calculated as the sum of the *Sync PTD (average)* and *Delay req. PTD (average)*. It is an estimation of the average time invested by a two-way IEEE 1588 packet transmission based on the packets collected from the beginning of the test. The *Two-way PTD (average)* is computed in slave emulation mode and in test mode.

Table 9.7: IEEE 1588 Delay Statistics

Result	Description
Asymmetry (current)	This result is computed as the difference of the *Sync PTD (current)* and *Delay req. PTD (current).* Delay asymmetry may cause a wrong time estimates in PTP slave clocks and for this reason this parameter has to be carefully controlled in PTP roll-outs for phase and time applications. This metric is computed both in slave emulation mode and in test mode.
Asymmetry (minimum)	This result is computed as the difference of the *Sync PTD (minimum)* and *Delay req. PTD (minimum).* This metric is computed both in slave emulation mode and in test mode.
Asymmetry (maximum)	This result is computed as the difference of the *Sync PTD (maximum)* and *Delay req. PTD (maximum).* This metric is computed both in slave emulation mode and in test mode.
Asymmetry (average)	This result is computed as the difference of the *Sync PTD (average)* and *Delay req. PTD (average).* This metric is computed both in slave emulation mode and in test mode.
Sync IAD (current)	Current Inter Arrival Delay (IAD) computed over the *Sync* packets received from a remote IEEE 1588 master clock. The Sync IAD is defined as the delay between two consecutively received IEEE 1588 Sync packets. The *Sync IAD (current)* metric is computed in slave emulation, pseudo-slave emulation (*test mode*) and passive monitor modes.
Sync IAD (average)	Mean value of the Sync IAD computed over all *Sync* messages received from the beginning of the test and expressed in microseconds. The *Sync IAD (average)* metric is computed in slave emulation, pseudo-slave emulation (*test mode*) and passive monitor modes.

Table 9.7: IEEE 1588 Delay Statistics

Result	Description
Sync correction (current)	Current value of the correction field found in received Sync messages. This value corresponds with correction field found in the last decoded Sync message. The *Sync correction (current)* metric is computed in slave emulation, pseudo-slave emulation (*test mode*) and passive monitor modes.
Sync correction (maximum)	Maximum value of the correction field found in a *Sync*registered from the beginning of the test. The *Sync correction (maximum)* metric is computed inslave emulation, pseudo-slave emulation (*test mode*) and passive monitor modes.
Sync correction (average)	Mean value of all the Sync correction field computed over all received Sync messages from the beginning of the test. The *Sync correction (average)* metric is computed in slave emulation, pseudo-slave emulation (*test mode*) and passive monitor modes.

1. From the *Home* panel, go to *RESULTS*,
   The test port results panel isdisplayed.
2. Select *Port A* to enter in the port specific results.
3. Enter in *PTP* to display results about the PTPprotocol.
4. Go to *Delay statistics*.
5. Press *Run* to start a new test and check the values of *Sync PTD (current)*, *Sync PTD (minimum)*, *Sync PTD (maximum)*, *Sync PTD (average)*, *Sync PTD (std. dev.)*, *Sync PTD (range)*, *Sync PDV (current)*, *Sync PDV (maximum)*, *Sync PDV (average)*, *Delay req. PTD (current)*, *Delay req. PTD (minimum)*, *Delay req. PTD (maximum)*, *Delay req. PTD (average)*, *Delay req. PTD (average)*, *Delay req. PTD (std. dev.)*, *Delay req. PTD (range)*, *Two-way PTD (current)*, *Two-way PTD (minimum)*, *Two-way PTD (average)*, *Asymmetry (current)*, *Asymmetry (minimum)*, *Asymmetry (maximum)*, *Asymmetry (average)*, *Sync IAD (current)*, *Sync IAD (average), Sync correction (current), Sync correction (maximum), Sync correction (average)*.

9.2.5. Clock Status

When the test unit is operating in slave emulation mode it is required to track the frequency and phase of a signal generated by a PTP master and encoded in different types of messages. Not ideal conditions in the master, the transmission network and the slave cause transient or permanent phase and frequency errors in the clock recovered by the slave equipment. These errors can be estimated on the basis of fluctuations no the received phase. The phase and frequency errors are displayed in the *Slave clock status* panel. To display the phase and frequency errors, follow these steps:

Table 9.8: Slave Clock Status Metrics

Result	Description
PTP time	If the unit is operating as a PTP grandmaster, this field shows the system time, which is the time the unit distributes to the remote PTP slaves. In PTP slave emulation mode, this field displays the time and date recovered from the grandmaster in the correct time scale as long as there is enough information to do that. The PTP time is not available if the unit is operating as a pseudo-slave (*Test* mode) or as a PTP monitor (*Monitor* mode)
Timescale	The *Timescale* defines how time is accounted by the device. The PTP protocol supports two different time scales: • *PTP*: This time scale is continuous and based on the SI second in the same way that the *International Atomic Clock* (TAI) time. The epoch (time origin) is defined to be 01/01/1970 00:00:00 TAI. • *Arbitrary*: Constitutes a continuous time scale with an epoch defined by an administrative procedure external to the PTP protocol. If the unit is configured in master emulation mode this field displays the current time scale being distributed by the test unit. In slave emulation mode this field shows the time scale inherited from the grandmaster.
UTC Offset	If the time scale is *PTP*, this field displays the offset between the UTC and the PTP (TAI) time. In January 2017 the UTC offset is 37 seconds.
Frequency offset	Displays the frequency offset between currently selected IEEE 1588 grandmaster and the test unit. If the equipment is working in slave emulation or passive monitoring modes, it slowly tracks the frequency recovered from the master. In this case, under ideal transmission conditions, the *Frequency offset* should converge to an small value. If the equipment is operating in pseudo-slave emulation (*Test* mode). This result corresponds with the offset between the frequency recovered from the grandmaster and the clock reference frequency.

Table 9.8: Slave Clock Status Metrics

Result	Description
Phase offset	Phase offset between the currently selected IEEE 1588 master and Tempo. If the equipment is working in slave emulation mode, it tracks the phase recovered from the master (and compensates for transmission latency using either the *Delay request-response* or the *Peer delay* mechanisms). The phase offset should be close to zero under ideal or nearly ideal transmission conditions. In pseudo-slave emulation mode (*Test* mode*)*, the phase offset shows the phase difference between the reference and the PTP signal. If the reference does not contain time information, the phase information is greyed out.

1. From the *Home* panel, go to *RESULTS*,
   The test port results panel is displayed.
2. Select *Port A* to enter in the port specific results.
3. Enter in *PTP* to display results about the PTP protocol.
4. Go to *Clock status*.
5. Press *Run* to start a new test and check the values of *PTP Time*, *Timescale*, *UTC offset* and *Frequency offset* and *Phase offset*.

9.2.6. Unicast Negotiation Results

If the equipment has been configured to use the unicast addressing model (See section 9.2.1), users are allowed to see the active signalling leases that enables the endpoint to transmit and receive miscellaneous PTP messages. To verify the unicast PTP leases follow these steps:

1. From the *Home* panel, go to *RESULTS*,
   The test port results panel is displayed.
2. Select *Port A* to enter in the port specific results.
3. Enter in *PTP* to display results about the PTP protocol.
4. Go to *Unicast negotiation.*
5. Select either *Outgoing leases* to see the message exchange leases initiated by the device or *Incoming leases* to see the leases initiated by the peer.
6. Check the *Clock id*. *Port*, *Address* and *Status fields* corresponding each PTP peer.
7. Scroll up or down to one of the table rows and select to display details about a particular unicast peer.
8. Check the *Message type*, *Interval* and *Status* for each row in the table

9.3. The Pseudo-slave Emulation Mode

The pseudo-slave emulation is similar to the slave emulation mode but the test unit now keeps an independent synchronization source. Typically, a GNSS reference is used but the test equipment could use any other reference such as ToD, 1 PPS, frequency inputs or even the internal oscillator in holdover / free running states. From the outside, the pseudo-slave and slave emulation modes are indistinguishable but internally they are different. Now, the reference and test signals can be compared and the measurement bandwidth could be extended to very low frequencies involving phase variations of hours or days typical of wander tests. If a time reference such as GNSS is used the *Time Error* (TE) could be computed as well. Finally, the pseudo-slave operation mode is also compatible with background traffic generation. This feature could be used to check any change in the TE, MTIE and TDEV depending on the traffic load. Additionally, some special test metrics such as the Floor delay population test require previous configuration of this PTP operation mode.

The pseudo-slave test mode is compatible both with the *IP endpoint* and the *Ethernet endpoint* operation modes. If the test is to be run in *IP endpoint* mode, the user is required to configure a valid IP profile (See section 9.2.1). Once the local profile has been configured the steps to follow to enable the pseudo-slave mode are described below:

1. Configure the clock reference input (See section 2.6).
2. From the *Home* panel, go to *TEST*,
   The test configuration panel is displayed.
3. Go to *PTP (IEEE 1588)*.
4. Configure the equipment to become a PTP pseudo-slave entity by configuring *PTP test* to *Test*.
   A label with the text PTP is displayed in the top notification area.
5. Set the transport protocol to either *Ethernet* or *UDP*.
   Note: If you are operating in *Ethernet endpoint* mode, the *UDP* transport protocol is not allowed.
6. Configure the *Addressing mode* to *Unicast*, *Multicast* or *Hybrid* depending on the system where the test unit is to be connected.
7. Depending on the PTP profile implemented in your system, configure *Path delay mechanism* to either *End-to-end* or *Peer-to-peer*.
8. Configure the *Domain* to the right value for your network.
9. If you have configured *Addressing mode* to *Unicast*, then you can configure one or more PTP entities to communicate with from the *Unicast master table* menu
   Note: Remote PTP entities are configured through their IP or MAC address, depending on the *Transport protocol.*
10. Configure the timing of the different messages associated to PTP from the *Message timing* menu.

9.3.1. TE Test

The basic performance parameter for phase and time deployments is TE. Basically, TE tells how much time a certain clock is ahead or behind some reference time. TE is generated in PTP-aware and non-PTP-aware network entities. Moreover, the transmission medium could also contribute to the TE. There are two mechanisms that could potentially generate TE:

- *Due to limited PRTC performance*, the time distributed through the network may not be accurate. If the PRTC is in holdover status an additional phase offset is expected to happen. This offset will be propagated to all the equipments locked to the PRTC.
- *Due to path delay asymmetry* the master-to-slave and the slave-to-master propagation delays may not be the same. It is not difficult to see that the TE generated by path asymmetry is one half of the value of the asymmetry. For example if the master-to-slave latency is 1 μs different compared with the slave-to-master latency, then the induced TE in the PTP slave will be 500 ns.

To measure the TE you have to configure the PTP pseudo-slave (*Test*) mode in your test unit. The only clock reference input that is compatible with the TE test is *GNS*S Once the equipment is configured in pseudo-slave mode, follow these steps:

1. From the *Home* panel, go to *RESULTS*,
   The test port results panel is displayed.
2. Select *Port A* to enter in the port specific results.
3. Enter in *PTP* to display results about the PTP protocol.
4. Go to *Time error statistics*
5. Start a test with the help of *run*.
6. Check the *Current*, *Maximum* and *Minimum* values corresponding with the *Total, Constant* and *Dynamic* TE.

Table 9.9: TE Statistics

Result	Description
Total	*Total TE*. This result accounts for the difference in time units between the time carried by the signal under test minus the reference. Computing the *Total* TE requires a time reference. The references currently available for this purpose are GNSS and ToD. *Current, Minimum* and *Maximum* figures are computed for the total TE. The minimum and maximum values are referred to the whole test duration.

Table 9.9: TE Statistics

Result	Description
Low frequency	*Low frequency Time Error*. This result expresses TE components that are immune to filtering. Such TE components are the result of, for example, asymmetry in the transmission medium between network elements or asymmetries within network elements. The low frequency TE spans the frequency band between 0 and 0.1 Hz. Constant (0 Hz) TE could theoretically be compensated through a static setting in the slave equipment, but slowly varying TE with periods of hours or days is both difficult to compensate or filter and it therefore should be avoided as much as possible. *Current, Minimum* and *Maximum* figures are computed for the low frequency TE. The minimum and maximum values are referred to the whole test duration.
High frequency	*High frequency Time erro*r. High frequency component of the TE. It is related to random noise accumulation due to packet-delay variation experienced by the timing signal packets or due to any other phase noise source. The power spectrum of the high frequency TE is spread out over the frequencies larger than 0.1 Hz and the power can be reduced, to some extent, through low-pass filtering. *Current, Minimum* and *Maximum* figures are computed for the dTE. The minimum and maximum values are referred to the whole test duration.

9.3.2. Wander (MTIE / TDEV) Test

Wander in a digital signal is defined as a slow phase fluctuation that degrades the quality of the clock embedded in the signal. The upper limit to the wander frequency band is usually defined to be 10 Hz but wander could have periods of hours or even days. Wander is propagated through the network and because it is not absorbed or filtered, it is accumulated impairing the timing signal. This concept of phase fluctuation could be translated without relevant modifications to synchronization protocols for packet switched networks such as PTP / IEEE 1588v2.

Measuring wander to assess the long term stability of a timing signal involves the use of an accurate clock reference due to the inability to filter out wander components from the signal under test. The phase of the reference clock is then compared with the phase corresponding to the signal under test. Performance metrics are then derived from the phase error. There are many performance figures defined to assess the quality of a timing signal but the most important of them are:

- The *time interval error* (TIE) is the phase fluctuation amplitude, which means that it indicates the phase variation of the clock to be measured, relative to the phase of an ideal reference clock during each measurement instant. The time origin, TIE=0 is taken as a reference at the start of the measurement. The TIE is expressed in absolute time units (ns, μs, ms).
- The *maximum time interval error* (MTIE) is the maximum value of peak-to-peak TIE in a certain observation time. This means that in order to calculate the MTIE, a time window of predefined length, *k*, must be scrolled over the function TIE (*n*), recording the maximum peak-to-peak value of the TIE. This can be repeated for different values of *k*, thus obtaining a graph of MTIE (*k*).
- *Time deviation* or TDEV is a measurement that characterizes the spectral content of a TIE (*n*) signal. This means that it measures the power of wander frequency components. The TDEV converges for all common types of phase noise, which makes it possible to identify the source and eventually correct the causes of degradation in transmission. As it is the case with MTIE, the TDEV is a function of the observation time *k*.

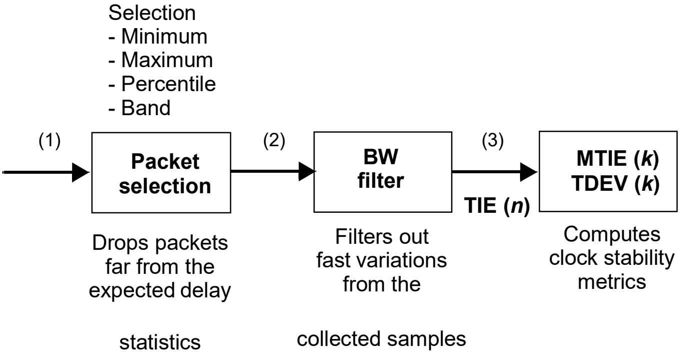


Figure 9.4: Wander measurement mechanism. The timing information has to be filtered before being delivered to the MTIE and TDEV block.

In digital circuits (PDH, SDH, SONET) the wander is always measured over the recovered clock. As the wander cannot be filtered out by the clock recovery circuit, the results are not affected by this test mechanism but on the other hand the unwanted fast phase fluctuations are removed or greatly attenuated. When dealing with PTP, wander can be evaluated directly from the packet interface but with this procedure the results are unrealistically pessimistic. The reason is that a real PTP slave clocks implement several packet selection and filtering mechanisms to improve the synchronization performance. ITU-T G.8260 defines several filtering mechanisms to be applied to the test equipment that makes it possible for these equipments to emulate the way commercial devices process and filter the PTP messages.

Tempo measures the *pktFilteredTIE*, *pktFilteredMTIE* and *pktFilteredTDEV* in the terms defined in ITU-T G.8260. The IEEE 1588 MTIE / TDEV is compatible with the *Ethernet endpoint* and *IP endpoint* operation modes (See section 2.1).

Table 9.10: Wander Test Configuration Parameters

Setting	Description
Enable	Enables or disables the PTP wander test. Wander tests can be executed only if PTP test has been configured to *Wander test.*
Observation time	Maximum window length for MTIE and TDEV results. The measurement is automatically stopped when the observation time is reached. Currently allowed values for the Observation time are 100 s, 1000 s, 10000 s, 100000 s and 1000000 s. *Note*: An MTIE / TDEV measurement may stop before reaching the maximum observation time if the autostop setting is configured to a value below the observation time. A critical error such a loss of clock reference or a loss of signal also stops the test.
Metric	Configures the performance metrics to be used in the next PTP wander test. The only option available in the current release is *pktFilteredTDEV / MTIE*. This option corresponds with the *pktFilteredMTIE* and pktFilteredTDEV as they are defined in ITU-T G.8260. The pktFilteredMTIE and pktFilteredTDEV are similar to their counterparts for TDM networks, the MTIE and TDEV, but these are computed directly in a packet interface.
Selection method	Configures one of the packet selection method to be used to filter PTP samples to compute wander performance metrics. The selection method configured in this field constitutes a not linear filter applied to the timing input before it is transferred to the wander metric calculation block. This filtering is used to discard samples and avoid unrealistic wander results. For example the filter could be used to discard packets with potentially more delay variation. The selection methods supported by the test units are defined in ITU-T G.8260 and they are listed below:

Table 9.10: Wander Test Configuration Parameters

Setting	Description
	• *Minimum:* Selects the packet with smaller end-to-end delay within the filtering window. • *Maximum:* Selects the packet with larger end-to-end delay within the filtering window. • *Percentile*: Uses a percentile value expressed in % to configure the packets to be processed by the MTIE / TDEV block (*Max. percentile*). Packets with an end-to-end delay larger than the configured percentile are not taken into account. • *Band*: Uses two percentile values expressed in % to configure the packets to be processed by the MTIE / TDEV block (*Max. percentile*, *Min. percentile*). Samples with a delay smaller than *Min. percentile* or larger than *Max. percentile* are ignored by the MTIE / TDEV block.
Selection window length	Configures the length of the not linear sample selection filter in seconds. Longer selection filters may potentially generate more accurate results but they involve an increase in the test period or at least in the amount of time required to get the first results
Min. percentile	Minimum allowed percentile in *Band* selection modes.
Max. percentile	Maximum allowed percentile in *Percentile* and *Band selection* modes.
BW filter window	Window length expressed in seconds for the linear filtering processing block placed before the MTIE and TDEV block. Unlike the selection filter, the linear filtering operates by averaging sample values before they are used to compute the MTIE and TDEV values. With this operation, it is pretended to simulate the behaviour of a real timing synchronization circuit that always tends to average the samples on its input. The BW filter window length is subject to the same kind of trade off that than the selection window. The longer the window the more accurate results but longer windows involve longer test periods as well.
Mask source	Configures the origin of the MTIE and TDEV masks to be used in the next measurement. The only currently allowed mask source is *Standard*, that configures the MTIE / TDEV mask from an ITU-T or an ETSI standard

Table 9.10: Wander Test Configuration Parameters

Setting	Description
Device type	Specifies which device or interface is to be tested. There are five potential choices for this setting: *E1 / T1 ITU Masks*, *PRC / PRTC ITU Masks*, *SEC / EEC ITU Masks*, *SSU ITU Masks*, *PTP ITU Masks*.
Standard	Selects the MTIE and TDEV mask to be used in the next measurement when Mask source is set to *Standard*. The list of masks available for selection depends on the current configuration of Device type: • T1 / E1 ITU Masks. This group contains the *PDH G.823*, *E1 TRF G.823*, *T1 TRF G.824*, *T1 REF G.824*, *PDH G.8261 CES 2048 kb/s (1)*, *PDH G.8261 CES 1544 kb/s (1)* and *PDH G.8261 CES (2A)*. • PRC / PRTC Masks. These are the *PRC G.811, ePRC G.811.1, PRC G.823*, *PRC G.824*, *PRC EN 300 462-3-1, PRTC-A G.8272 Locked mode, PRTC-B G.8272 Locked mode* and *ePRTC G.8272.1* masks. • SEC / EEC ITU Masks: *SEC G.823, SEC G.813 / EEC G.8262 Constant Temperature (1)*, *SEC G.813 / EEC G.8262 Constant Temperature (2)*, *SEC G.813 Holdover (2)*, *SEC G.813 / EEC G.8262 Noise tolerance (1)*, *SEC G.813 / EEC G.8262 Noise tolerance (2)*, *SEC G.813 Noise transfer (2)*, *SEC G.813 Ref. sw. / EEC G.8262 Phase disc. (2), SEC G.813 / EEC G.8262 Variable temperature (1)*. *EEC G.8261 (1)*, *EEC G.8261 (2)* and *EEC G.8261 Noise transfer (2)*. • SSU ITU Masks: These are the *SSU G.823*, *SSU G.812 Noise Generation I (CT)*, *SSU G.812 Noise generation II, III (CT)*, *SSU G.812 Noise tolerance*, *SSU G.812 Noise Generation (VT)*, *SSU G.812 Noise transferI*, *SSU G.812 Noise transfer II, III.*. • PTP ITU Masks: *PEC G.8261.1 (3)*, *PEC G.8263 Constant temperature*, *PEC G.8263 Variable temperature*, *PTP G.8271.1 Reference point C*, *BC G.8273.2 dTE A, B (CT), BC G.8273.2 dTE C (CT)*. Pass / Fail results are computed by comparison of the test results and the configured mask value

To measure the TE you have to configure the PTP pseudo-slave (*Test*) mode in your test unit. Any clock reference input, including time, phase and frequency references are compatible with the MTIE / TDEV test. Once the test unit is configured in pseudo-slave mode, follow these steps:

1. From the *Home* panel, go to *TEST*,
   The test configuration panel is displayed.
2. Go to *PTP wander test.*
3. Enable the MTIE / TDEV test by setting the *Enable* control to *On*.
4. Configure the *Observation time*, to one of the allowed values. The test finishes automatically when the *Observation time* is reached.
5. Optionally, configure the packet selection filter through the *Selection method*, *Selection window length*, *Min. percentile* and *Max. percentile* settings.
6. Optionally, configure the low pass filter by means the *BW filter window* control.
7. Configure the *Mask source, Device type* and *Standard mask* parameters for the next MTIE / TDEV measurement.

The unit is now ready to run the test and read the results. To do that, this is the correct procedure:

1. From the *Home* panel, go to *RESULTS*,
   The test port results panel is displayed.
2. Select *Port A* to enter in the port specific results.
3. Enter in *PTP* to display results about the PTP protocol.
4. Go to *PTP wander test*.
5. Choose between *MTIE* or *TDEV.*
6. Start the test by pressing *Run*.
7. Check the *Time*, *TIE*, *MTIE* and *Mask* results (*MTIE* results panel) or *Time*, *TDEV* and *Mask* results (*TDEV* results panel).
   Note: The TIE, MTIE and TDEV values must be understood as pktFilteredTIE, pktFilteredMTIE, and pktFilteredTDEV respectively.
   Note: The amount of time to wait before the first results are displayed depends of the filter settings.

9.3.3. Floor Delay Population Test

PTP slave clocks may increase their accuracy and stability by implementing packet selection mechanisms. In simple terms, this means that it is an advantage for PTP slave clocks to just discard packets with a potentially large amount of phase error rather than trying to use them in any way.

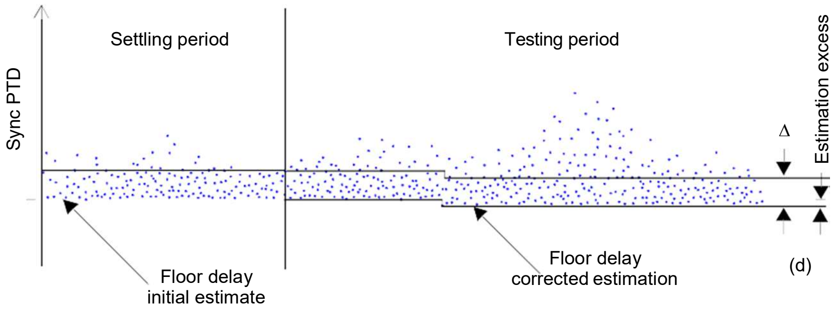


Figure 9.5: Illustration of the floor delay population test. Samples are classified as conforming or not conforming depending on the latency they experience from the grandmaster.

The floor delay population test attempts to implement a mechanism to measure the number of samples suitable for slave synchronization. With this objective in mind, the test defines an acceptable end-to-end delay range. The lowest delay is defined to be the floor delay for the path under test. In other words, the smallest time recorded for a packet as it is transmitted through the path. The highest delay is obtained by adding a fixed time to the floor delay. Samples are rated as conforming if they are found between the minimum and the maximum delay. Not conforming packets exhibit an end-to-end delay larger than the maximum. By definition, there are no packets with end-to-end delay below the floor delay.

Tempo implement the floor delay population with the equipment configured in pseudo-slave mode. The procedure to configure the equipment in this mode is the same that for the MTIE / TDEV test (See section 9.3.2). If the equipment is configured in *IP endpoint* mode, configuration of a IP profile is also necessary. This configuration is also identical to the MTIE / TDEV test (See section 9.3.2). Once the IP profile, the external reference and the pseudo-slave mode are all configured, these are the steps to follow to run the floor delay population test:

1. From the *Home* panel, go to *TEST*,
   The test configuration panel is displayed.
2. Go to *Floor delay population test (FPP).*
3. Configure *Enable* to *On* to activate the test
4. Enter the value of the *Min. delay settling time* if you want to modify the floor delay calculation period.
5. Configure the *FPC window length* if you want to modify the time window to compute the FPC, FPR and FPP metrics.

6. Modify the values of *FPC delta* and *FPP threshold* to change the default pass / fail threshold for the FPP.

Table 9.11: Floor Delay Population Test Configuration Parameters

Setting	Description
Enable	Enables or disables the PTP floor delay population test. Wander tests can be executed only if PTP test has been configured to *Wander test.*
Obs. floor delay method	It determines the procedure to measure the floor delay. The only floor delay measurement method available today is *Progressive*. The *Progressive* mechanism evaluates the floor delay along the whole testing period but there is an initial period of configurable length that is used to do a first estimate of this parameter. In order to get the maximum accuracy in the test results, the observed floor delay during the settling period has to be as exact as possible. Variations of the floor delay after the settling period are computed as an estimation excess. Results are therefore less accurate as the estimation excess becomes larger.
Min. delay settling time	Amount of time devoted to compute the floor delay. Longer values for this setting contribute to a more accurate estimation of the floor delay and therefore higher quality in the test results.
Overall min. floor delay	This configuration field is not used in the current implementation of the floor delay population test.
FPC window length	The floor delay population method is based on a sliding window mechanism. The relevant metrics are referred to a time window that changes its position in time. The FPC window length configures the floor delay population test sliding window length. ITU-T G.8261.1 uses a window length of 200 s to specify the network operation limits.
FPC delta	Configured the delay excess from the floor delay used to determine the conformity of a received sample. ITU-T G.8261 uses a delta of 150 μs to specify the operation network limit
FPP threshold	This parameter is the ratio of conforming samples to the total amount of received samples. ITU-T G.8261.1 state that at least 1% of the received samples should be within a 150 μs range accounted from the floor delay computed for the path.

Table 9.12: Floor Delay Population Results

Result	Description
FPC (pkts)	*Floor Packet Count* (FPC). This is the amount of conforming packets received within the current window. This count is updated once per second as new samples are received and the test window moves through the time axis. ITU-T Recommendations do not currently supply any network operation limit based on the FPC metric.
FPR (pkts/s)	The *Floor Packet Rate* (FPR) corresponds with the amount of conforming samples received per unit time. ITU-T Recommendations do not currently supply any network operation limit based on the FPR metric.
FPP (%)	The *Floor Packet Percentage* (FPP) is the ratio of conforming samples to received packets expressed as a percentage. ITU-T G.8261 specifies an FPP of 1% or smaller for a delta of 150 μs and a test window of 200 s.
Estimated floor delay	This result field is not used in the current implementationof the floor delay population test.
Observed floor delay	This result field is not used in the current implementationof the floor delay population test.
Estimation excess	The *Estimation excess* is the difference between the floor delay computed in the initial settling period and the smallest observed delay during the test period. Ideally, the *Estimation excess* should be 0. A value different to 0 implies that the initial floor delay estimation was not accurate. A large estimation excess may involve a partial accuracy loss in the test results.
Floor delay estimation	This field reports a possible loss of accuracy due to a wrong estimation of the floor delay.
Sync packet rate	The *Sync packet rate* field reports modifications on the Sync message packet rate during the current test. Message rate modifications affect the test results and must be avoided during the testing period.

Once the test has been configured, follow these steps to run the measurement and read the results:

1. From the *Home* panel, go to *RESULTS*,
   The test port results panel is displayed.
2. Select *Port A* to enter in the port specific results.

3. Enter in *PTP* to display results about the PTP protocol.
4. Go to *Floor delay population test (FPP)*.
5. Press *run* to start a new test
   Note: On the top right corner a *Settling* indication is displayed at the beginning of the test. Once the settling period expires the indication changes to Testing but no result is displayed before the measurement window is filled with data.
6. Check the values of *FPC (pkts)*, *FPR (pkts/s)* and *FPP (%)*.
7. Verify that the *Estimation excess*, the *Floor delay estimation* and *Sync packet rate* are acceptable.

9.4. PTP Passive Monitoring

Sometimes, the ability to qualify the operation of an existing PTP slave already connected to the network is more important than a full emulation of a PTP slave. A typical example happens when an slave device exhibits poor performance for unknown reasons. A quick PDV measurement with Tempo could be useful to determine whether the problem is caused by the network (congestion, inappropriate switches) or the device (high sensitivity to PDV, configuration problem).

The passive monitoring operation mode is defined so that it doesn’t affect the network in any way. No PTP traffic is generated in this mode. Interaction is limited to analysis of the different types of messages received from other PTP master and slave clocks. Connection in Ethernet or IP endpoint is allowed when the monitoring mode is configured but the *IP through* mode is allowed as well. By connecting the equipment in pass-through mode at the output of the DUT (usually a PTP slave) it is possible to analyse the messages the DUT is receiving without any intermediate device that could be masking the real synchronization performance.

When the test unit is operating in *PTP monitor* mode it cannot track the phase generated by the master because it does not estimate the path delay (Delay request-response mechanism, Peer-delay mechanism) but it can still syntonize the master frequency. The result is that all metrics related with absolute phase or delay are not available in PTP *Passive monitor* mode.

If you want to run the PTP monitor in *IP endpoint* or *IP through* modes, you will need to set your local profiles with correct IP addresses, network masks and gateways. For the specific case of the *IP through* mode, you will have to configure the local profile of both *Port A* and *Port B*. The details are as follow:

1. From the *Home* panel, go to *CONFIG*
   The test port settings panel is displayed.
2. Select *Port A* to enter in the port specific configuration.

3. Configure the *local profile* (See section 2.3) either by means the DHCP protocol or by hand.

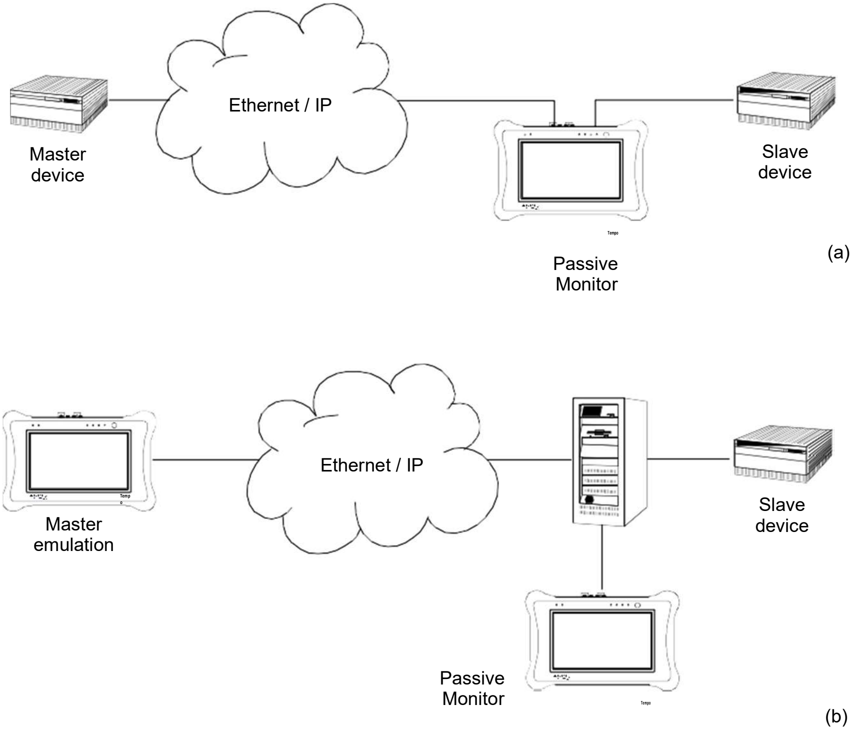


Figure 9.6: Connection of Tempo to the network in PTP *Passive monitor* mode: (a) Connection in pass-through mode (IP through operation mode). (b) Connection in endpoint mode (*Ethernet endpoint* or *IP endpoint* operation modes).

If your operation mode is *IP endpoint*, the local profile configuration finishes here. If you are working in *IP through* mode, repeat the previous steps for *Port B*. The configuration specific for the PTP protocol is detailed in the following steps:

1. From the *Home* panel, go to *TEST*,
   The test configuration panel is displayed.
2. Go to *PTP (IEEE 1588)*.
3. Configure the equipment to become an passive IEEE 1588 monitor by configuring *PTP test* to *Monitor*.
   A label with the text PTP is displayed in the top notification area.
4. Set the transport protocol to either *Ethernet* or *UDP*.
   Note: If you are operating in Ethernet endpoint mode, the *UDP* transport protocol is not allowed.

5. Configure the *Domain* to the right value for your network. The default value in most networks is 0.
6. Go to *Master identity* to select a remote PTP master clock.
7. Configure Source of identity to one of the allowed values: *Auto*, *IPv4 address*, and *Host name* (UDP transport protocol) or *Auto* and *MAC address* (*Ethernet transport* protocol).
8. If you have configured *Source of identity* to *IPv4 address*, *Host name* or *MAC address*, fill the correct master identify field with the data from yourmaster.
9. Optionally, configure the timing of the different messages associated to PTP from the Message timing menu.

Once configured, you can use the same measurement procedures described for the PTP master and slave clock emulation (See section 9.2) to get statistics and counts in your test environment. The only difference in the results is that in the *Passive monitor* mode only a subset of the statistics available for the endpoint emulation are available.

9.5. NTP Server and Client Emulation

Tempo has the capability to emulate either an NTP server or a client Theoretically, there is no difference between any standard NTP clock or the testers but the latter supply measurement results that are useful to qualify the stability of NTP timing sources, the network performance when delivering different kinds of NTP messages and the ability of NTP clients to recover an accurate timing from the messages they receive from their masters:

When the equipment is configured as an NTP client or server, Tempo provides three different kinds of result with many common points with the PTP results in master / slave emulation mode:

- *Protocol state*: Not specifically test results. The protocol state contains details reported by the server clock when the unit is configured in NTP client emulation mode or about the client if configured in NTP server emulation mode.
- *Message statistics*: Includes message counts classified by their type (*Client* messages, *Server* messages, *Control* messages...).
- *Delay statistics*: Reports some quantities defined by NTP standards and particularly by RFC 5905 such as theta (the time offset), delta (round trip delay) and psi (jitter). The RFC 5905 results are complemented by some otherproprietary

parameters related with delay and latency such as the forward and return path delay or the asymmetry.

Table 9.13: NTP Configuration

Setting	Description
NTP mode	Configures the NTP test to be executed. These are the options currently available for this setting: • *None*: Disables all NTP generation and analysis. • *Client*: Choose this mode if you want the test unit to behave as a NTP client clock. The unit becomes a new NTP client in your network it will generate and receive traffic in the same way than any other NTP clock installed in your network once it is properly configured. • *Server*: Choose this mode if you want the test unit to behave as a NTP server clock. The unit becomes a new NTP server in your network it will generate and receive traffic in the same way than any other NTP clock installed in your network once it is properly configured. • *Test*: Configures the unit as an NTP pseudo-client that behaves in the same way than any standard NTP slave but doesn't get synchronization from the an NTP server but from a clock reference chosen by the user. This is the correct operation mode to run a NTP TE test.
Version	Configures the version of the NTP protocol to be used to exchange information with the peer server or client clocks. Two versions are supported: version 3 (*NTPv3*), which is defined by RFC 1505 and version 4 (*NTPv4*), from standard RFC 5905
Server IPv4 address from	Establishes the origin of the destination IPv4 address for the current stream. There are three different settings available for configuration: • *Manual*: The NTP sever address is set to the value configured in *Destination IPv4 address*. • *Host name*: Uses the Domain Name Service (DNS) to set the NTP server IP address by using descriptive alphanumeric strings. The DNS mechanism requires intervention of at least one DNS server. The DNS server IP address has to be configured in the Port A local port profile either statically or by means DHCP (See section 2.3).

Table 9.13: NTP Configuration

Setting	Description
Server host name	Domain name to be used as NTP server identity if *Server IPv4 address from* is set to *Host name*. Unlike IP addresses, domain names are easy-to-remember alphanumeric strings but they have to be translated to IP addresses before any packet can be sent to the destination. The translation process requires the intervention of at least one DNS server. The DNS server IP address has to be configured in the local port profile either statically or by means DHCP (See section 2.3).
Server IPv4 address	Server IPv4 address configured if *Server IPv4 address from* is set to *Manual*. The address is entered in decimal, four-dotted format. Any address between 0.0.0.0 and 255.255.255.255 is admitted as a destination IPv4 address.
Server IPv4 address (DNS)	Destination IPv4 address carried by the packets generated in the current stream if *Destination IPv4 address from*is set to *Host name*. This is a read only field that it cannot be edited directly. It displays the result of the DNS name resolution carried out with the host name configured in *Server host name.*
Minimum polling interval	Minimum allowed polling interval in client (and pseudo-client) emulation mode. NTP clients generate queries to servers periodically and they are allowed to change the polling rate within a user configurable range. Typically, clients set the polling range to a higher speed initially but once they achieve steady operation they can slow down the packet exchange rate.
Maximum polling interval	Maximum allowed polling interval in client (and pseudo-client) emulation mode. NTP clients generate queries to servers periodically and they are allowed to change the polling rate within a user configurable range. Typically, clients set the polling range to a higher speed initially but once they achieve steady operation they can slow down the packet exchange rate.

Table 9.13: NTP Configuration

Setting	Description
Hold time (s.)	The Hold time (s.) setting configures the period of time the equipment devotes to estimate the frequency offset between the local host and the server. The longer the time, the more accurate the estimate. Usually, larger values of this setting are required in noisy channels with high packet delay variation During the hold time period the local clock is not adjusted and therefore some large frequency and / or phase offset may be measured in the test unit.
Time properties	Configures the values of certain fields related with timing sources of the time and / or frequency signal generated by the test equipment when it is configured in NTP server emulation mode.

The NTP client and server clock emulation is only compatible with the *IP endpoint* operation mode (See section 2.1). Before running the NTP emulation mode you need to configure your local profile. To do that, the required steps are:

1. From the *Home* panel, go to *CONFIG*
   The test port settings panel is displayed.
2. Select *Port A* to enter in the port specific configuration.
3. Configure the *Local profile* (See section 2.3) either by means the DHCP protocol or by hand.

To run the NTP test follow these steps:

1. From the *Home* panel, go to *TEST*,
   The test configuration panel is displayed.
2. Go to *NTP*.
3. Configure the equipment to become an active NTP entity by configuring *NTP mode* to *Client* or *Server*, depending on the role you want to achieve.
   A label with the text *NTP C* (for Client) or *NTP S* (for server) is displayed in the top notification area.
4. In server emulation mode, Configure the protocol *Version* to *NTPv3* or *NTPv4* and, optionally, the *Time properties*. Skip this step in client emulation configurations
5. In client emulation mode, configure the server address either through a host name or an IP address through the *Server Pv4 address from*, *Server host name* and *Server IPv4 address* fields. Skip this step in server emulation mode.
   Note: Host name resolution requires the configuration of a DNS server in the IP local profile. The IP address resulting for the DNS resolution is displayed in *Server IPv4 address (DNS)*.

6. In client emulation mode, configure the *Minimum polling interval*, *Maximum polling interval* and *Hold time (s.)* to control the message exchange and locking process timings.

It must be taken into account that when the equipment is configured in client emulation mode the timing is derived from the NTP messages it receives from the test interface. Any external reference such as GNSS or 1 PPS is ignored and could bedisabled. When the unit is configured to run in master emulation mode the time to be distributed is obtained from the external reference if the time is available (GNSS, ToD, IRIG-B). With phase references (1 PPS) the NTP phase is still aligned with the reference but only the local system time could be distributed. With frequency references (2048 kHz, 2048 kb/s, 1544 kHz, 1544 kb/s, 10 MHz) both the phase alignment and the time are internally generated from the system clock but the NTP signal is still syntonized with the reference frequency.

Table 9.14: NTP Time Properties Settings

Setting	Description
Mode	It is one of *Manual* or *Auto* • *Manual*: The user decides the value of the time properties fields and flags. This setting is required if detailed debug of the NTP server-to-client association is required. • *Auto*: Lets the test unit decide which settings to usefor the time properties. Using *Manual* time properties does not make sense if the unit is not operating in NTP server emulation mode. For this reason, this control is configured statically to *Auto* in slave emulation and in test modes.

Table 9.14: NTP Time Properties Settings

Setting	Description
Type of Stratum	Configures the type of stratum in the local NTP server. The stratum can be used to specify where an NTP clock located in the synchronization hierarchy. Primary servers, are assigned stratum 1. These clocks corresponds with the roots of the synchronization tree. Stratum 1 clocks feed secondary clocks structured in different levels so that stratum 2 get their time from stratum 1, stratum 3 are synchronized from stratum 2, etc. Stratum 0 and 16 have special meanings. The Type of Stratum field can be configured to any of the following values: • *Unspecified*: Corresponds with a stratum value of 0 and this is the value to be configured in invalid servers or when the stratum cannot be specified for any reason. • *Primary*: Configures the server as a primary (stratum 1) clock. These clocks report their quality level through special alphanumeric codes configured in the *Reference ID* field. • *Secondary*: Configures the server as a secondary (stratum 2 -15) clock. Secondary clocks get their synchronization either from primary clocks or from other secondary clocks of higher stratum level than their own. • *Unsynchronized*: Configures the server as an stratum 16 clock corresponding with a not synchronized clock.
Reference ID from	Assigns a Reference ID for a primary clock. This field can be configured to any of the following values. • *Auto*: Lets the system assign a reference ID automatically based on the current clock reference and other status and configuration variables: • *Predefined*; Configures the *Reference ID* to any of the predefined codes listed in RFC 5905. If this option is selected then users must choose a value from *Reference ID*. • *Custom*:: Lets the user decide their own custom Reference ID from any alphanumeric string with length smaller or equal of four characters..

Table 9.14: NTP Time Properties Settings

Setting	Description
Reference ID	Configures the NTP clock Reference IDin primary and secondary clocks. For primary clocks users are allowed to choose between any of the following identifiers: • *GOES*: Geosynchronous Orbit Environment Satellite • *GPS*: Global Position System • *GAL*: Galileo Positioning System • *PPS*: Generic pulse-per-second • *IRIG*: Inter-Range Instrumentation Group • *WWVB*: LF Radio WWVB Ft. Collins, CO 60 kHz • *DCF*: LF Radio DCF77 Mainflingen, DE 77.5 kHz • *HBG*: LF Radio HBG Prangins, HB 75 kHz • *MSF*: LF Radio MSF Anthorn, UK 60kHz • *JJY*: LF Radio JJY Fukushima, JP 40 kHz, Saga, JP 60 kHz • *LORC*: MF Radio LORAN C station, 100 kHz • *TDF*: MF Radio Allouis, FR 162 kHz • *CHU*: HF Radio CHU Ottawa, Ontario • *WWV*: HF Radio WWV Ft. Collins, CO • *WWVH*: HF Radio WWVH Kauai, HI • *NIST*: NIST telephone modem • *ACTS*: NIST telephone modem • *USNO*: USNO telephone modem • *PTB*: European telephone modem • *Custom*: Custom code. A character string not longer than four characters. This option is possible only if *Reference ID from* is configured to *Custom*. In secondary clocks the reference ID is the IPv4 address corresponding to the NTP server where the current device is retrieving synchronization information. The address is entered in decimal, four-dotted format.

Table 9.14: NTP Time Properties Settings

Setting	Description
Kiss Code	If the stratum level is set to 0, then the kiss code can be used to convey debug or other useful information. These are the Kiss codes defined by RFC 5905: • *ACST*: The association belongs to a unicast server. • *AUTH*: Server authentication failed. • *AUTO*: Autokey sequence failed. • *BCST*: The association belongs to a broadcast server. • *CRYP*: Cryptographic authentication or identification failed. • *DENY*: Access denied by remote server. • *DROP*: Lost peer in symmetric mode. • *RSTR*: Access denied due to local policy. • *INIT*: The association has not yet synchronized for the first time. • *MCST*: The association belongs to a dynamically discovered server. • *NKEY*: No key found. Either the key was never installed or is not trusted. • *RATE*: Rate exceeded. The server has temporarily denied access because the client exceeded the rate threshold. • *RMOT*: Alteration of association from a remote host running ntpdc. • *STEP*: A step change in system time has occurred, but the association has not yet resynchronized.
Stratum	Configures the stratum in NTP secondary servers. It could be any number between 2 and 15.

Table 9.14: NTP Time Properties Settings

Setting	Description
Leap status	Configures a custom value for the leap seconds status field when the tester is running in server emulation mode. The allowed options are listed below: • *Auto*: Let's the system determine the reported leap seconds status based on the information it retrieves other clock reference inputs. • *None*: This is the value reported when no leap second events are planned for the current day. • *61 seconds*: Reports that one leap second will be added to the last minute of the current day. As a result the last minute will have 61 seconds. • *59 seconds*: Reports that one leap second will be deleted at the and of the last minute of the current day. As a result he last minute will have only 59 seconds • *Unknown*; No information about leap seconds is available in the NTP server.

9.5.1. Protocol State

The basic NTP results are available in the *Protocol State* panel. All the information contained in this panel is collected from messages received from remote NTP entities or is an indication of the state of the internal NPT synchronization machine. For this reason, the results depend on whether the unit is running in server or client emulation modes.

The *Protocol State* results are permanent, it is not required to start a test (*RUN* button) to display the information from this panel. The information is updated in real-time as new changes in the protocol state are registered by the test unit. To display the protocol state panel follow these steps:

1. From the *Home* panel, go to *RESULTS*,
   The test port results panel is displayed.
2. Select either *Port A* to enter in the port A specific results.
3. Enter in *NTP* to display results about the NTP protocol.
4. Go to *Protocol state* and check *Port state*, *Local Stratum, Local Reference ID, Local Leap status*, *Polling interval*, *Peer Stratum*, *Peer Reference ID*, *Peer Root*

Delay, *Peer Root Dispersion*, *Peer Leap status*, *Local NTP time* and *Peer NTP time.*

Table 9.15: Protocol State Results

Result	Description
Port state	Displays the current port state which defines how is currently behaving the equipment and its ability to generate requests or process replies from the peer. It is any of the following: • *Listening*: The port is ready to accept and reply to client requests. This port state applies to NTP servers only. • *Invalid*: The port is not able to generate an NTP request. One explanation to this state is that the underlying protocol layers have not been properly configured. For example, the network interface may lack of a correct IP profile with at least an IP address and subnet mask. • *No answer*: The port has generated a request directed to a remote NTP server but the server has not replied to this request. This port state applies to NTP clients only. • *Non-acceptable response*: The NTP client has received an invalid answer from the server. The reason to declare a server message as non-acceptable could be due to the packet formatting, an out of range value in some packets fields or any other reason that prevents proper processing or the received message. • *Delaying time step*: This is a message that is displayed when the NTP client that is running in the port detects a sudden change in the time received from the server. Once this situation arises the client waits for a period of time to avoid a time step due to transient perturbations that could degrade the server time for a limited period of time. • *Adjusting frequency*: The NTP client is receiving and processing server messages and it is using the information contained in these messages to adjust the internal oscillator frequency. The frequency adjustment is required before the equipment could start working adjusting time.Typically NTP will adjust the frequency for a user configurable period of time before entering in the next state where the frequency will remain locked to the server. • *Adjusting time*: This is an state declared in the NTP client after once the frequency adjustment has finished and it corresponds with the normal steady operating conditions of the NTP client port.

Table 9.15: Protocol State Results

Result	Description
	• *Testing*: This is an special port state reported when Tempo is running a test in the port. This state does not correspond with the normal frequency / time adjusting states because in test mode timing information is collected from an external reference not from NTP.
Local stratum	NTP domains are structured in a layered structure where every layer is known as an stratum. A number is assigned to each stratum. For example, stratum 2 clients get their synchronization from stratum 1, stratum 3 from stratum 2, etc. The top stratum level, stratum 1 servers are synchronized through a mechanism that is out of the scope of the NTP standard such as GPS, LORAN or other means.
Local reference ID	Reports the reference ID corresponding with the local clock. It could be an alphanumeric code (primary clocks) or the IP address from the server where the clock is synchronized to (secondary server).
Local leap status	It warns about pending leap second events. These are the possible settings for this field: are: • *None*: This is the value reported when no leap second events are planned for the current day. • *61 seconds*: Reports that one leap second will be added to the last minute of the current day. As a result the last minute will have 61 seconds. • *59 seconds*: Reports that one leap second will be deleted at the and of the last minute of the current day. As a result he last minute will have only 59 seconds • *Unknown*; No information about leap seconds is available in the NTP server.
Polling Interval	Current polling interval in client (and pseudo-client) emulation mode. NTP clients generate queries to servers periodically and they are allowed to change the polling rate within a user configurable range. Typically, clients set the polling range to a higher speed initially but once they achieve steady operation they can slow down the packet exchange rate.
Peer stratum	In client emulation mode or test (pseudo-client) mode, it reports the peer stratum. If the local stratum is not overriden by a custom user configuration, then it is determined by the peer stratum. Specifically, the local stratum in a

Table 9.15: Protocol State Results

Result	Description
Peer reference ID	In slave emulation mode or in test mode it reports the reference ID corresponding with the peer clock. It could be an alphanumeric code (primary clocks) or the IP address from the server where the clock is synchronized to (secondary server).
Peer root delay	This value is an estimate of the delay from the primary clock server computed and reported by the peer. This value accumulates through the server chain from the primary (stratum 1) clock.
Peer root dispersion	This value is an estimate of the delay dispersion from the primary clock server computed and reported by the peer. This value accumulates through the server chain from the primary (stratum 1) clock.
Peer leap status	Leap seconds status reported by the peer when the equipment is configured in client emulation mode or in test mode.
Local NTP time	Time generated by the NTP entity running in the local machine. If the unit is running in master emulation mode, the local NTP time matches the time the server is distributing to remote clients. This time is obtained either from an external reference and if no suitable reference is available then it is internally generated. In client emulation mode the local time is obtained from the NTP master clock. Finally, in test mode (pseudo-client mode) the local NTP time corresponds with a time provided by an external time reference (GNSS, ToD or IRIG-B).
Peer NTP time	In slave emulation or in test mode this field reports the time reported by a remote NTP server.

9.5.2. Message Statistics

The *Message statistics* panel include counts of each NTP message type defined in RFC 1305 and RFC 5905. This result panel includes statistics both about received and transmitted (internally generated) packets. The procedure to display the message statistics is as follows:

1. From the *Home* panel, go to *RESULTS*,
   The test port results panel is displayed.
2. Select either *Port A* to enter in the port A specific results.
3. Enter in *NTP* to display results about the NTP protocol.
4. Go to *Message statistics*.

Press *Run* to start a new test and check the transmitted (TX) and received (RX) values of *Symmetric active*, *Symmetric passive*, *Client*, *Server*, *Broadcast, Control* and *Other* message types.

Table 9.16: Message Statistics

Result	Description
Symmetric active	Accounts for the number of received (RX) and transmitted (TX) *Symmetric active* messages. Symmetric active messages are generated if the NTP peers communicate through the symmetric variant. This operation mode allows NTP entities to provide time to its peers and also to request timing information from them. This is appropriate in configurations involving a number of redundant time servers interconnected through diverse network paths. Active time servers exchange messages with other active servers but they may also generate requests to servers with no specific active associations. In this case, they can respond through ephemeral associations mobilized upon the arrival of the request and demobilized upon error or timeout.
Symmetric passive	Accounts for the number of received (RX) and transmitted (TX) *Symmetric passive* messages. Like it happens with Symmetric active messages, Symmetric passive messages are generated in symmetric communications between NTP peers. However, unlike Symmetric active messages, these are generated by ephemeral associations generated in hosts to respond to Active Symmetric messages.
Client	Number of received (RX) and transmitted (TX) NTP *Client* messages. Client messages are generated when the NTP host communicate through the client / server variant. An NTP client pulls synchronization from the server by generating requests to the server and accepting the replies to these messages.
Server	Accounts for the number of received (RX) and transmitted (TX) NTP *Server* messages. Server messages are also used in the client / server communications. Servers provide information to one or more clients by responding request messages by Server response packets but they don’t accept timing information from them.

Table 9.16: Message Statistics

Result	Description
Broadcast	Number of received (RX) and transmitted (TX) NTP *Broadcast* messages. Broadcast NTP servers send messages to clients periodically. Clients willing to accept broadcast messages generate ephemeral broadcast associations to process this information. The broadcast model is uncommon compared with the symmetric and client / server modes because it is inherently less accurate and secure than the alternatives.
Control	Total number of received (RX) and transmitted NTP control messages. Control messages are used to configure NTP entities when no other resources such as the SNMP protocol are usable.
Other	Accounts for the total number of received (RX) or transmitted (TX) NTP messages not belonging to any of the previous types.

9.5.3. Delay Statistics

Many of the delay statistics computed by Tempo correspond with values required by the NTP time tracking algorithm to keep the accurate time estimates based on the information received from one or more servers. The values are displayed by the tester as they are calculated following the rules from the standards. Specifically, RFC 5905 is used for time offset, round-trip delay and jitter statistics. Since offset / latency do not need to be tracked by NTP servers, these values are not available when test mode is set to server emulation.

There are three statistics the NTP time tracking mechanism is not able to calculate with the resources provided by the protocol: *Delay (forward)*, *Delay (return)* and *Asymmetry*. For this reason, these statistics are only given in NTP test mode which is an operation mode specifically designed for the purpose of generating accurate estimates of client-to-server and server-to-client delay statistics together with other metrics derived from these. To display statistics about delay and time offset, follow these steps:

1. From the *Home* panel, go to *RESULTS*,
   The test port results panel is displayed.
2. Select *Port A* to enter in the port specific results.
3. Enter in *NTP* to display results about the NTP protocol.
4. Go to *Delay statistics*.
5. Press *Run* to start a new test and check the values of *Offset (theta)*, *Delay (delta)* and *Jitter (psi)*.

6. If you are running the NTP test mode (See section 9.6) check the values of *Delay (forward)*, *Delay (return)* and *Asymmetry*.

Table 9.17: Delay Statistics

Result	Description
Offset (theta)	The time *Offset*, referred by the NTP standards with the Greek θ (theta) letter represents the maximum-likelihood time offset of the server clock relative to the system (client) clock. The time offset parameter displayed here is computed following the specification give in RFC 5905 This is a parameter that is adjusted by the client at every step of the disciplining algorithm based on message arrival times and the time stamps carried by NTP messages. The clock disciplining process tracks the server time by configuring its own time to the value that provides a minimum offset.
Delay (delta)	The *Delay (delta)* represents the round-trip delay from the NTP server to the client The delay parameter is computed following the specification from RFC 5905. The round trip delay is adjusted by NTP clients every time a new message is received. Delay estimates enable clients to compensate for variable or fixed propagation delay from the NTP servers that would generate an error in the client.
Delay (forward)	The *Delay (forward)* accounts for the propagation delay from the NTP server to the client. Together with Delay (return), makes up the round-trip delay Accurate estimates of Delay (forward) require an external independent time reference which is only available when *NTP mode* is configured to *Test*. Specifically, forward and return path delay measurements are not available NTP client emulation mode.
Delay (return)	The *Delay (forward)* accounts for the propagation delay from the NTP client to the server. Together with Delay (return), makes up the round-trip delay Accurate estimates of Delay (return) require an external independent time reference which is only available when *NTP mode* is configured to *Test*. Specifically, forward and return path delay measurements are not available NTP client emulation mode.

Table 9.17: Delay Statistics

Result	Description
Asymmetry	This result is computed as the difference of *Delay (forward)* and *Delay (backward).* This result, which is closely related with 2-way TE estimates is important to know how good is the network delivering time through the NTP protocol Accurate estimates of Delay (return) require an external independent time reference which is only available when *NTP mode* is configured to *Test*. Specifically, forward and return path delay measurements are not available NTP client emulation mode.
Jitter (psi)	The *Jitter (psi)* is defined as the root-mean-square (RMS) average of the most recent offset differences, and it represents the nominal error in estimating the offset. The jitter is computed following the specification from RFC 5905.

9.6.NTP Pseudo-client Mode

The pseudo-client emulation is similar to the client emulation mode but the test unit now keeps an independent synchronization source. Typically, a GNSS reference is used but the test equipment could use any other time reference such as ToD or IRIG-B. It is also possible to run a pseudo-client test in holdover. From the outside, the pseudo-slave and slave emulation modes are indistinguishable but internally they are different. Now, the reference and test signals can be compared and the measurement bandwidth could be extended to very low frequencies involving phase variations of hours or days typical of wander tests. If a time reference such as GNSS is used the *Time Error* (TE) could be computed as well. Finally, the pseudo-client operation mode is also compatible with background traffic generation. This feature could be used to check any change in the TE depending on the traffic load.

The pseudo-client test mode is compatible with *IP endpoint* operation modes only. The user is required to configure a valid IP profile (See section 9.5).Once the local profile and the reference has been configured the steps to follow to enable the pseudo-client mode are described below:

1. Configure the clock reference input (See section 2.6).
2. From the *Home* panel, go to *TEST*,
   The test configuration panel is displayed.
3. Go to *NTP*.
4. Configure the equipment to become a NTP pseudo-client entity by configuring *NTP mode* to *Test*.
   A label with the text NTP C (for client) is displayed in the top notification area.

5. Configure the server address either through a host name or an IP address through the *Server Pv4 address from*, *Server host name* and *Server IPv4 address* fields. *Note*: Host name resolution requires the configuration of a DNS server in the IP local profile. The IP address resulting for the DNS resolution is displayed in *Server IPv4 address (DNS)*.
6. Configure the *Minimum polling interval*, *Maximum polling interval* and *Hold time (s.)* to control the message exchange and locking process timings.

9.6.1. TE Test

The most important performance metrics in any time distribution application is the 2-way TE and related results, which accounts for the difference between the time provided by the application and a (supposedly perfect) reference. This is the approach from ITU-T G.810 that defines performance parameters useful to rate timing and synchronization applications.

Table 9.18: TE Results

	Description
Current	*Current TE.* This result accounts for the difference in time units between the time carried by the signal under test minus the reference. The definition of Time Error follows standard ITU-T G.810. Computing the *Current* TE requires a time reference. The references currently available for this purpose are GNSS, ToD and IRIG-B.
Average	*Average TE*. This result accounts for the average TE value computed over all the samples collected from the beginning of the test.
Minimum	*Minimum TE*. This result accounts for the minimum TE value computed over all the samples collected from the beginning of the test.
Maximum	*Maximum TE*. This result accounts for the maximum TE value computed over all the samples collected from the beginning of the test.
Standard deviation	*TE standard deviation*. This results accounts for the standard deviation of all samples collected from the beginning of the test.

To measure the TE you have to configure the NTP pseudo-client (*Test*) mode in your test unit. The clock reference inputs compatible with the TE test are *GNSS*, ToD and IRIG-B. Once the equipment is configured in pseudo-client mode, follow these steps:

1. From the *Home* panel, go to *RESULTS*,
   The test port results panel is displayed.
2. Select *Port A* to enter in the port specific results.
3. Enter in *NTP* to display results about the NTP protocol.
4. Go to *Time error statistics*
5. Start a test with the help of *run*.
6. Check the *Current*, Average, *Maximum* and *Minimum* and *Standard deviation* results corresponding with the *Total* 2-way Time error.

Chapter 10 Synchronous EthernetAnalysis

Tempo may optionally support the ITU-T defined Synchronous Ethernet standard which enables these equipments qualify Synchronous Ethernet network equipment or to generate Ethernet signals synchronized to various timing sources, including GPS and TDM.

10.1.Introduction to Synchronous Ethernet

Synchronous Ethernet is an ITU-T standard that provides mechanisms to transfer frequency over the Ethernet physical layer, which can then be made traceable to an external source such as a network clock. As such, the Ethernet link may be used and considered part of the synchronization network.

The proposal to specify the transport of a reference clock over Ethernet links was brought by operators to ITU-T Study Group 15 in September 2004. The aim of Synchronous Ethernet is to avoid changes to the existing IEEE Ethernet, but to extend it working within its protocol definitions.

Despite being an IEEE standard, Ethernet architecture has been described in ITU-T G.8010 as a network made up of an ETH layer and a ETY layer. Put in simple terms, the ETY layer corresponds the physical layer as defined in IEEE 802.3, while the ETH layer represents the pure packet layer. Ethernet MAC frames at the ETH layer are carried as a client of the ETY layer. In OSI terminology, ETY is layer 1, ETH layer 2. Synchronous Ethernet is based on the ITU-T G.8010 description of the Ethernet architecture.

A key topic in Synchronous Ethernet is the definition of the mechanisms necessary to achieve interworking between SDH / SONET and Synchronous Ethernet equipment. These mechanisms and procedures are found fundamentally in three different recommendations: ITU-T G.8261, G.8262 and G.8264. The aspects covered there include the following:

- Extension of the synchronization network to include Ethernet as a building block (ITU-T G.8261). This enables Synchronous Ethernet network equipment to be connected to the same synchronization network that SDH /SONET. Synchronization for SDH /SONET can be transported over Ethernet and the opposite is also true.

- The ITU-T G.8262 defines Synchronous Ethernet clocks compatible with SDH / SONET clocks. Synchronous Ethernet clocks are based on ITU-T G.813 clocks and they are defined in terms of accuracy, noise transfer, holdover performance, noise tolerance, and noise generation. These clocks are referred as Ethernet Equipment Slave clocks. While the IEEE 802.3 standard specifies Ethernet clocks to be within ±100 ppm. EECs accuracy is within ±4.6 ppm. Additionally, by timing the Ethernet clock, PRC traceability of the interface is achievable.
- ITU-T G.8264 extends the usability of the ITU-T G.707 Synchronization Status Message (SSM) by Synchronous Ethernet equipment. The SSM contain an indication of the quality level of the clock that is driving the synchronization chain. The *Ethernet Synchronization Message Channel* (ESMC) is used for propagation of the SSM through the Synchronous Ethernet network.

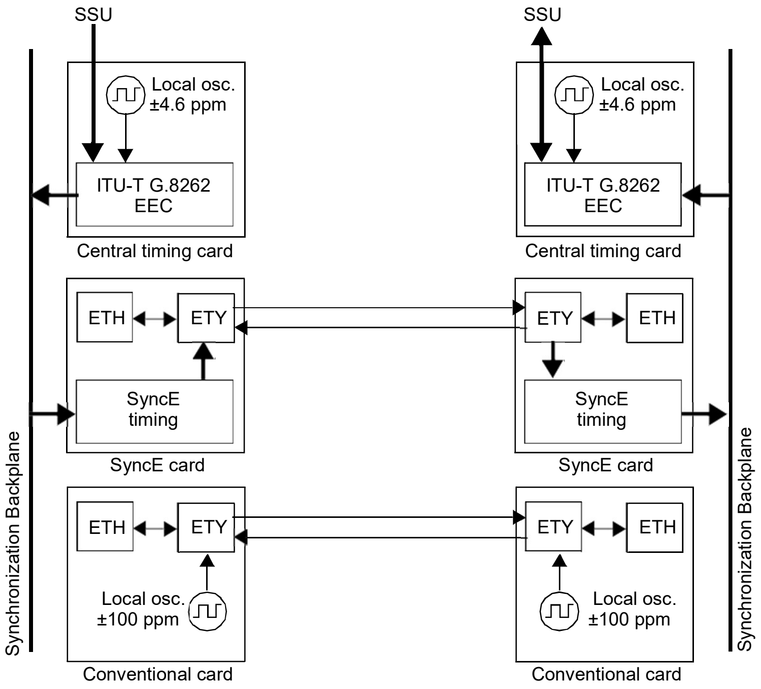


Figure 10.1: Synchronous Ethernet Architecture and comparison with conventional Ethernet

The basic difference between a conventional Ethernet and a Synchronous Ethernet network interface card is that the Synchronous Ethernet card is prepared to accept external timing or to supply timing to other subsystems. On the other hand, the conventional card is relegated to operate with its own ±100 ppm internal clock. Note that the conventional card is still able to use the clock from an external subsystem (for example the CPU) for data transmission but data reception is not coupled to the transmitter clock and it is also uncoupled to other transmitters in the network. This last feature is the one that defines IEEE 802.3 Ethernet as an asynchronous technology.

Synchronous Ethernet ability to accept or give timing signal makes this technology suitable for hierarchical synchronization. Here, the key element is the EEC which enables Ethernet nodes to accept or supply synchronisation to other Ethernet or TDM equipments. Thanks to this property, Synchronous Ethernet becomes a new building block of the synchronization network.

10.1.1. Ethernet Synchronization MessagingChannel

In SDH / SONET, the SSM provides traceability of synchronization signals and it is therefore required to extend the SSM functionality to Synchronous Ethernet to achieve full inter operability with SDH equipment.

In SDH, the SSM message is carried in fixed locations within the SDH frame. However, in Ethernet there is no equivalent of a fixed frame. The mechanisms needed to transport the SSM over Synchronous Ethernet are defined by the ITU-T in G.8264 in cooperation with IEEE. More specifically, the ESMC, defined by the ITU-T is based on the Organization Specific Slow Protocol (OSSP), currently specified in IEEE 802.3ay.

The ITU-T G.8264 defines a background or *heart-beat* message to provide a continuous indication of the clock quality level. However, event type messages with a new SSM quality level are generated immediately.

The ESMC protocol is composed of the standard Ethernet header for a slow protocol, an ITU-T specific header, a flag field, and a type length value (TLV) structure. The SSM encoded within the TLV is a four-bit field whose meaning is described in ITU-T G.781.

10.1.2. Synchronous Ethernet for the 1000BASE-T Interface

Historically, the 1000BASE-T is the first Ethernet interface that makes use of advanced modulation and encoding technology to enable simultaneous full duplex transmission over four twisted pairs in Cat. 5 cables.

Another property that makes different the 1000BASE-T interface to other Ethernet interfaces such as 1000BASE-X or 100BASE-TX is synchronization. The 1000BASE-T modulation is not compatible with asynchronous operation. During the auto-negotiation process, 1000BASE-T peers decide which transmission end becomes the master and which is the slave. This basic synchronization mechanism is suitable to achieve synchronization in the 1000BASE-T link but is not a mechanism it can be used for global synchronization of the Ethernet network. In fact, the 1000BASE-T synchronization mechanism constitutes a limitation to the operation of Synchronous Ethernet. One link that is operating as a 1000BASE-T slave is unable to accept a timing signal from the EEC and thus is unable to accept an arbitrary timing source.

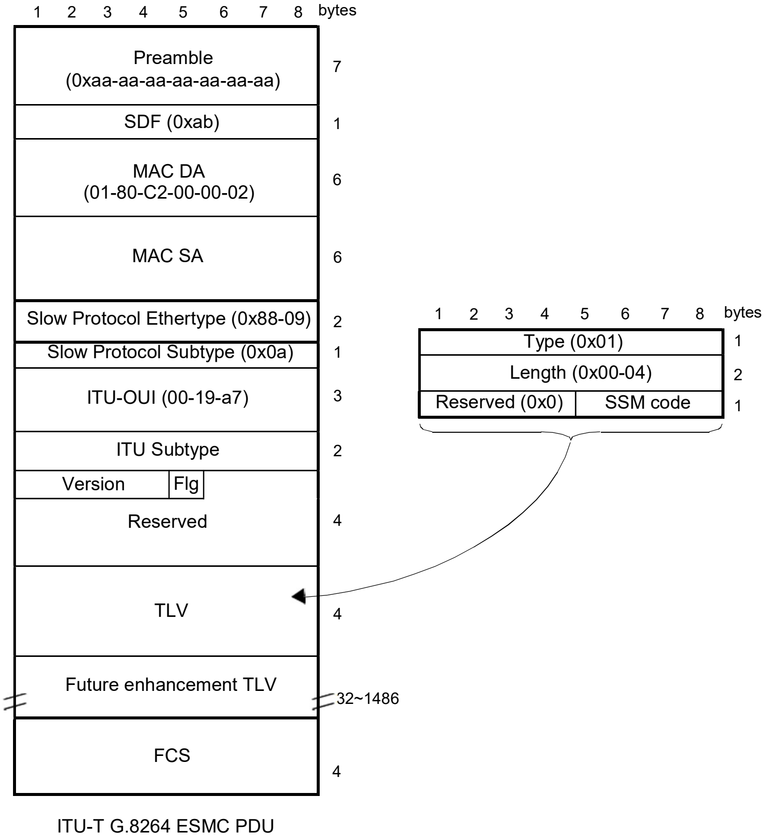


Figure 10.2: Ethernet Synchronization Message Channel (ESMC) protocol data unit.

This condition is different to other Ethernet interfaces where the transmission is synchronized to timing sources other than the reception clock and are therefore suitable to be added to a hierarchical synchronization network through the EEC without any special constrain.

Ethernet 1000BASE-T interfaces can still use Synchronous Ethernet, but the EEC is always required to be connected to the master while the slave is constrained to operate with the timing signal recovered from the master. The result is that synchronization of 1000BASE-T is always unidirectional and propagating from the master to the slave while in 1000BASE-X or 100BASE-T you can theoretically have one synchronization signal propagating in each transmission direction.

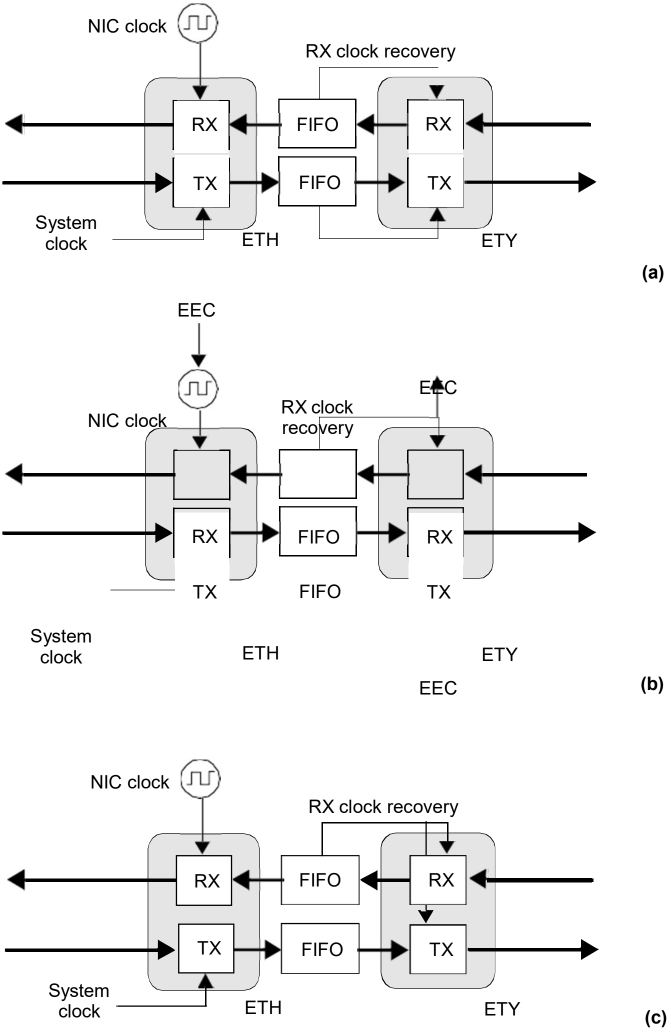


Figure 10.3: Ethernet synchronization models: (a) Conventional Ethernet. There are at least two clock domains. The transmitter and the receiver are in different clock domains (b) Synchronous Ethernet. All clocks are slaves of the EEC. The RX recovered clock could be used as an input for the EEC. (c) 1000BASE-T slave. The TX clock is always an slave of the RX clock.

10.2. Frequency Measurement

In conventional Ethernet, the received frequency is not a critical parameter as long as it is within the ±100 ppm range specified by the IEEE 802.3 standard. However, Synchronous Ethernet frequency is important because this frequency is used by external elements as a synchronization source. Tempo includes a frequency measurement that can be used to verify that the frequency offset of the received signal lies within acceptable limits. To enable the frequency measurement in the test unit, follow these steps:

1. Make sure that your tester is connected to the network. The physical layer must be up and working in the correct test interface (See section 4.1.1).
   Note: if you are measuring frequency over the 1000BASE-T interface, force the slave role in the test port by disabling *100-FD* and *10-FD* and configuring *Clock role* to *Slave* (See section 2.2.3).
2. From the *Home* panel, go to *Results*,
   The port setup panel is displayed.
3. Select either *Port A or Port B* to enter in the port specific results menu.
4. Go to Frequency.
5. Check the *Frequency* and *Frequency deviation* results.

If you need increased accuracy for your frequency test, you can use an external clock for measuring. Different kinds of clock inputs are accepted by the test unit, including TDM, frequency, 1PPS / ToD and GNSS sources (See section 2.6)

10.3. MTIE / TDEV Analysis

The Synchronous Ethernet wander test is in many aspects similar to the PTP / IEEE 1588v2 analysis (See section 9.3) and analogous to the E1 / T1 analysis (See the *E1 / T1 / Datacom / IEEE C37.94 Testing Guide*). The main difference with the PTP / IEEE 1588v2 test is that in Synchronous Ethernet there no need to explicit configuration of any packet selection mechanism or linear filter and therefore the pktFilteredTIE, pktFilteredMTIE and pktFilteredTDEV could be replaced by the traditional TIE, MTIE and TDEV. The difference with the E1 / T1 analysis is basically the operation frequency which is 1544 kHz / 2048 kHz for E1 / T1 wander tests and the Ethernet line frequency for Synchronous Ethernet. To configure and run an MTIE / TDEV test in a Synchronous Ethernet interface follow these steps:

1. Make sure that your tester is connected to the network. The physical layer must be up and working in the correct test interface (See section 4.1.1).
2. Connect and configure a clock reference in your test unit (See section 2.6).
3. From the *Home* panel, go to *CONFIG*
   The Port configuration panel is displayed.
4. Set operation mode to *Ethernet endpoint*, *IP endpoint* or *IP through*.

5. From the *Home* panel, go to *TEST*
   The test configuration panel is displayed.
6. In the *SyncE wander test* field, configure *MTIE / TDEV*.
7. Configure the *Observation time* to one of the allowed values. The test finishes automatically when the *Observation time* is reached.
8. Configure the *Mask source, Device type* and *Standard mask* parameters for the next MTIE / TDEV measurement.

The unit is now ready to run the test and read the results. To do that, this is the correct procedure:

1. From the *Home* panel, go to *RESULTS*,
   The test port results panel is displayed.
2. Select *Port A* to enter in the port specific results.
3. Enter in *SyncE wander* to display the Synchronous Ethernet synchronization results.
4. Go to *Wander analysis.*
5. Run the test by pressing the *run* key.
6. Check the *Overflow*, *TIE*, *Offset*, *Max. offset*, *Drift* and *Max. drift* results.
7. Leave the current panel and choose between *MTIE* or *TDEV.*
8. Check the *Time*, *TIE*, *MTIE* and *Mask* results (*MTIE* results panel) or *Time*, *TDEV* and *Mask* results (*TDEV* results panel).
   Note: MTIE and TDEV test results could be displayed either through a table or in graphical format with the help of *a* contextual button.

Table 10.1: Wander analysis results

Result	Description
Overflow	This is an indication about TIE measurement overflow. TIE dynamic range is ±2 s. If the phase excursion is higher than this value, the displayed TIE will not be correct. To indicate this condition, the *Overflow* field displays *Yes*.
TIE	Displays the current Time Interval Error (TIE). The TIE is the cumulative phase error from the beginning of the test. The allowed dynamic range for the TIE is ±2 s. Results out of this range will generate an overflow event.
Offset	Difference between the frequency of the received signal and the reference signal frequency measured in parts per million (ppm). Measurement of the frequency offset does not require to run a measurement. It is a permanent result that is available even if there is not an ongoing test.

Table 10.1: Wander analysis results

Result	Description
Max. offset	Maximum frequency offset registered from the beginning of the test. The sign is not considered when the maximum offset is computed. For example, if the measured offset values are between -4 ppm and +3 ppm, the recorded maximum offset will be -4 ppm.
Drift	Change rate of the frequency offset expressed in parts per million per second (ppm/s).
Max Drift	Maximum frequency drift registered from the beginning of the test. The sign is not considered when the maximum offset is computed. For example, if the measured drift values are between -4 ppm/s and +3 ppm/s, the recorded maximum drift will be -4 ppm/s

10.4. Frequency Offset Generation

Tempo can be used to impair the frequency of the test signal generated in test ports A and B with a frequency offset in the range of -125 ppm and +125 ppm. This test can be used to check how tolerant to frequency variations is a network element. Also, if you have a chain with various equipments transmitting a synchronization reference, you can replace the reference by the Tempo test signal and test the ability of the chain to transmit frequency variations to the last element of the chain. The configuration procedure for frequency offset generation over Ethernet interfaces is as follows:

1. Make sure that your tester is connected to the network. The physical layer must be up and working in the correct test interface (See section 4.1.1).
   Note: if you are generating frequency offset over the 1000BASE-T interface, force the master role in the test port by disabling *100-FD* and *10-FD* and configuring *Clock role* to *Master* (See section 2.2.3).
1. From the *Home* panel, go to *CONFIG*,
   The port setup panel is displayed.
2. Go to *Wander generator*.
3. Configure the *Frequency deviation (ppm)* with the frequency offset you want to generate between -125 and 125 ppm.
   Note: The frequency offset is generated in all ports operating in master mode at

the same time. Make sure that you are not generating any unwanted perturbation in a network interface.

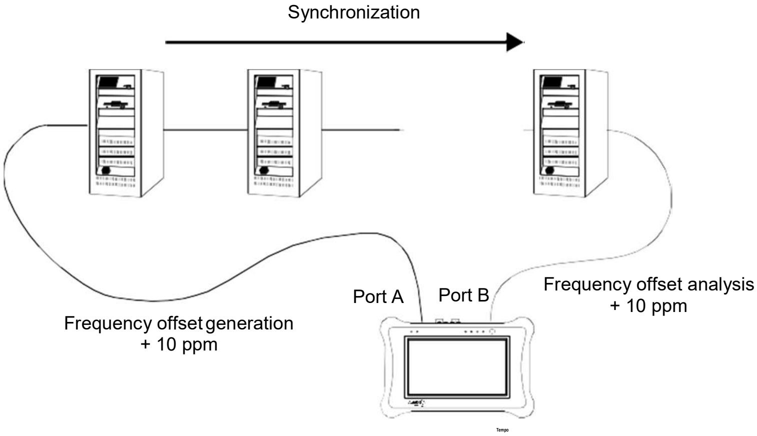


Figure 10.4: If Synchronous Ethernet is used for transmission of timing signals, network elements in the chain should be transparent to offset generation at its input and therefore any frequency offset should be recovered at the output of the chain.

10.5. Wander Generation

Wander generation can be used to stress network elements and see how phase modulation is accumulated as it is propagated through the network. To configure the wander generator follow these steps.

1. Make sure that your tester is connected to the network. The physical layer must be up and working in the correct test interface (See section 4.1.1).
2. If you are using an external timing reference, enable it (See section 2.6).
3. From the *Home* panel, go to *CONFIG*,
   The test port configuration panel is displayed.
4. Set operation mode to *Ethernet endpoint*, *IP endpoint* or *IP through*.
5. From the *Home* panel, go to *Test*
   The *Test* configuration panel is displayed.
6. Configure *SyncE wander test* to *Generation*.
7. Go back to *CONFIG*,
8. Go to the *Wander generator* menu.

9. Enable the wander generator by configuring *Wander generator* to *On*.
   An small *W* is displayed on the top of the screen to show that the wander generator has started working.
10. Set the *Modulation waveform* to *Sinusoidal*
   Note: *Sinusoidal* is the only waveform currently available for the wander modulating signal.
11. Configure the frequency and amplitude of the wander modulating signal.
   Note: Maximum amplitude depends on the frequency. Check the maximum amplitude allowed for the current frequency before setting the *Amplitude* field.

Table 10.2: Wander generation settings

Setting	Description
Frequency deviation (ppm)	Frequency offset applied to the transmitter clock within the range of ±125 ppm. This feature is useful to stress the DUT/ SUT.
Wander generator	Enables or disables the wander generator. If the generator is disabled, the Port A transmit signal will not contain any wander phase modulation. If it is enabled, the phase will be modulated by the signal specified by the *Modulation waveform*, *Amplitude (pp)* and *Frequency* controls.
Modulation waveform	Modulating signal to be applied to the phase of the test signal generated by the tester. The only one possible configuration for the modulating waveform is currently *Sinusoidal,* that sets an harmonic modulating signal.
Amplitude (pp)	Sets the peak-to-peak amplitude of the modulating signal in time units. The maximum allowed value for this field depends on the *Frequency*. You can configure higher amplitude values if the frequency is smaller.
Max. amplitude (pp)	This is an informative field that can not be set by the user. It displays the maximum peak-to-peak amplitude, expressed in time units, allowed for the *Amplitude (pp)* field. The maximum amplitude depends on the value of the *Frequency* field.
Frequency	Sets the frequency of the phase modulating signal in μHz, mHz or Hz.

10.6. Operation in IP Through Mode

You can use the test unit to forward and impair the Ethernet frequency in pass-through mode. Specifically, Tempo is capable of forwarding synchronization and traffic between port A and B and adding frequency offset to the signal forwarded to port A. The procedure to do that is as follows:

1. Make sure that your tester is connected to the network in pass-through mode. The physical layer must be up and working in ports A and B (See section 4.1.1).
   Note: if you are working with the 1000BASE-T interface, force the master role in the test *Port A* and slave role in test *Port B*. Also, you have to disable the *100-FD* and *10-FD* auto-negotiation options for both ports (See section 2.2.3).
2. From the *Home* panel, go to *CONFIG*,
   The test port setup panel is displayed.
3. Configure *Mode* to *IP Through*.
4. Go to *Reference clock*.
5. Configure *Input clock* to *Ethernet (Port B)*.
6. From the port setup panel, now go to *Wander generator*.
7. Configure the *Frequency deviation (ppm)* with the frequency offset you want to generate between -125 and 125 ppm.
   The unit adds an offset to the frequency detected in Port B. This offset is transmitted to test port A.

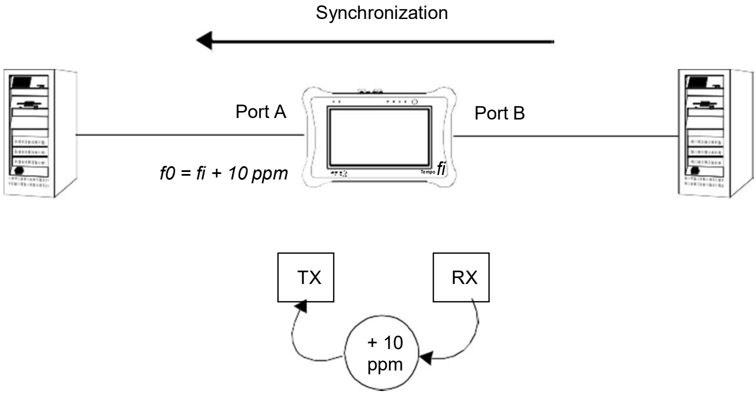


Figure 10.5: With the help of Tempo it is possible to generate frequency offset in pass-through mode to stress the network.

10.7. ESMC Generation and Analysis

The test unit can be configured to generate and analyse the ESMC in a Synchronous Ethernet interface. Specifically, Test ports are allowed both to generate and monitor the ESMC. The correct ESMC generation procedure is as follows:

1. Make sure that your tester is connected to the network. The physical layer must be up and working in the correct test interface (See section 4.1.1).
2. From the *Home* panel, go to *CONFIG*,
   The test port configuration panel is displayed.

3. Select *Port A* to enter in the port specific configuration.
4. Make sure that Port mode is configured to TX / RX
   Note: Depending on the unit global operation mode the TX / RX port mode may not be available. Specifically, you cannot configure *TX / RX* in *IP through* mode.
5. Enable the ESMC generation by configuring *Enable* to *Generation &* Analysis. ESMC generation starts from this moment
6. Configure the *ITU-T G.781* option (*Option I*, *Option II*, *Option III*) to assign labels to the SSM in accordance with your network. You can also set *ITU-T G.871* to *Custom* to configure the SSM in numeric format.
   Note: The *ITU-T G.871* setting is applied also to the decoding of the SSM received from the remote end.
7. Enter the correct SSM from the *Sync. status message (SSM)* control if you are configured *Option I*, *Option II* or *Option III* in ITU-T G.781 or through *Custom SSM* if you have configured *Custom* in *ITU-T G.781*.

The ESMC analysis procedure is slightly different. In order to configure it, follow these steps:

1. Make sure that your tester is connected to the network. The physical layer must be up and working in the correct test interface (See section 4.1.1).
2. From the *Home* panel, go to *CONFIG*,
   The test port configuration panel is displayed.
3. Select *Port A* or *Port B* to enter in the port specific configuration.
4. Make sure that *Port mode* is configured to *TX / RX* or *Monitor*.
5. Enable the ESMC analysis by configuring *Enable* to *Analysis* or *Generation & Analysis*.
   Note: *Generation & Analysis* also enables *ESMC* generation.
6. Configure the *ITU-T G.781* option (*Option I*, *Option II*, *Option III*) to decode the SSM in accordance with your network. You can also set *ITU-T G.781* to *Custom* to display the SSM in numeric format only.

Finally, if you have configured ESMC Generation & Analysis or ESM Analysis you can read the current SSM and other parameters from the test unit. This is the correct sequence to do that:

1. From the *Home* panel, go to *RESULTS*,
   The test port results panel is displayed.
2. Select *Port A* or *Port B* to enter in the port specific results.
3. Go to ESMC.
4. Start a test using *Run*.

5. Check the *Current QL*, *Current QL (hex)*, *Message count* and *Event count* parameters.

Table 10.3: ESMC analysis results

Event	Description
Current QL	Displays the ITU-T G.781 mnemonic corresponding to the current quality level received in SSM messages This result is referred to the last SSM message decoded by the test unit. The identifier displayed in this field depends on the *ITU-T G.781* settings. Labels are different for ITU-G G.781 Option I, Option II and Option III.
Current QL (hex)	Displays the hexadecimal code corresponding to the current quality level received in SSM messages. This result is subject to the same conditions that *Current QL* but it does not depend on the synchronization option (Option I, Option II or Option 3).
Message count	Shows the number of SSM packets received from the beginning of the test
Event count	Displays the number of SSM packets with the *Event* flag enabled received from the beginning of the test. The *Event* flag indicates a change in the QL and therefore this result could be used to account for the transitions occurred from the beginning of the test.

Chapter 11
GOOSE and SV Analysis

The IEC 61580 is a set of standards defined with the purpose of describing the building blocks of the communication network for modern digital power substations. IEC 61850 describes the substation communications protocols but its scope is much broader and it also covers the abstract modeling of substation components and their interactions. Moreover, the latest edition of the standard (edition 2) is not limited to substation communications and it also addresses substation to substation communications (IEC 61850-90-1) or communications between substation and the operation center (IEC 61850-90-2). IEC 61850 has become a global solution for power utility communications and it currently is the dominant standard for this application.

The prevalent protocols before the advent of IEC 61850 were based on low speed serial transmission (RS-232 and its cousins). The own IEC 61850 standard was initially conceived as a development of one of these protocols, IEC 60870-5, but during the discussion of the standard new ideas introduced significant modifications in the original schedule:

1. Use of *Ethernet transmission* to replace serial hard-wired interconnections in the substation. Ethernet provides a fast, cost effective transmission, often over an optical “bus”. This approach simplifies cabling and saves costs while improving manageability and versatility.
2. Use of *object oriented semantics* to describe the substation elements and their interactions. This approach offers a powerful tool to build abstract models of the substation functions at the process, bay and station levels and it is the basis to enable vendor interoperability.

The Calnex Tempo test unit has the ability to verify the performance of two of the most important protocols defined by IEC 61850: The *Generic Object Oriented Substation Events* (GOOSE) protocol and the *Sampled Values* (SV) protocol. The GOOSE and SV protocols are the basis of the communication between *Intelligent Electronic Devices* (IEDs) connected to the *Station bus* or the *Process bus* in a power substation.

The GOOSE and SV carry time sensitive information and the analysis of the time required by this protocols to be transmitted and propagated through the network to the destination becomes critical. Tempo carries out this analysis providing detailed time statistics required to assess the performance level of any IED or network based on GOOSE or SV protocols.

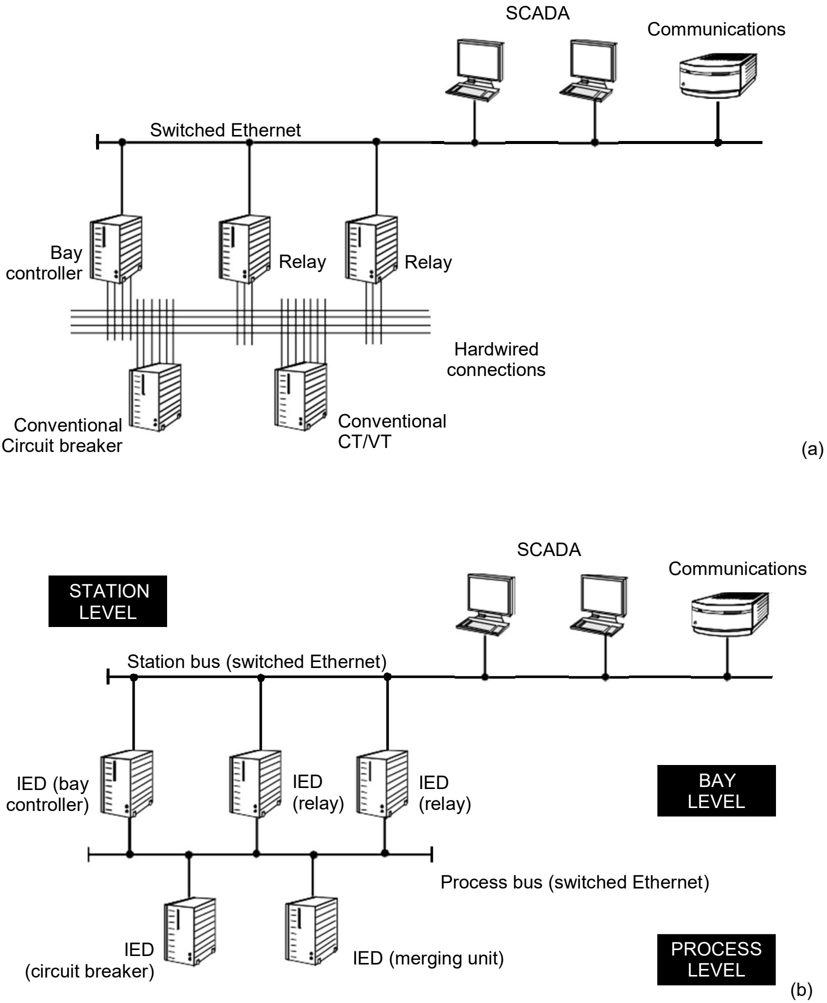


Figure 11.1: One of the advantages of Ethernet compared with serial communications and hard-wired binary inputs / outputs is that cabling is simpler, efficient and if optical fibre is used, transmission is immune to electromagnetic interferences. (a) In a conventional substation, even if a modern communications network could be used to interconnect the supervision and control subsystem with the bay level, the protection mechanism is largely based on binary signals transmitted over hard-wired connections. (b) IEC 61850 normalizes the station bus and replaces the hard-wired connections with a new (process) bus based on Ethernet communications to interconnect the bay and

process levels.

11.1. IEEE 61850 Performance Requirements

Defining the performance requirements for substation communications is the subject of IEC 61850-5. This standard defines seven *message types* with specific requirements on maximum latency and other performance metrics. Some message types are also subdivided in *performance classes* to account for different performance levels. For example, we have the 1A message type, which is the right type for trip protection messages, with three different performance classes: P1, P2 and P3. The latency requirement for class P1 is 3 ms and for classes P2 and P3 it is 10 ms.

Table 1: Time and latency requirements for IEC 61850-5 message types

Type	Description	Requirements
1A	Fast messages (trip)	• Transmission time (P1): 10 ms, • Transmission time (P2, P3): 3 ms
1B	Fast messages (other)	• Transmission time (P1): 100 ms • Transmission time (P2, P3): 20 ms
2	Medium speed messages	• Transmission time: 100 ms
3	Low speed messages	• Transmission time: 500 ms
4	Raw data messages	• Transmission time (P1): 10 ms, • Transmission time (P2, P3): 3 ms
5	File transfer functions	• Transmission time: 1000 ms
6	Time synchronization	*Protection and control:* • Accuracy (T1): 1 ms • Accuracy (T2): 100 µs *Requirements for instrument transformers:* • Accuracy (T3): ±25 µs • Accuracy (T4): ±4 µs • Accuracy (T5): ±1 µs
7	Command messages	Transmission time: 500 ms

Of the seven existing message types, type 1 (fast messages) is reserved for GOOSE, type 4 (raw data) is for SV and class 6 (time synchronization) applies to timing protocols such as PTP or NTP and also to timing sources such as GNSS. Message types 2, 3, 5 and 7and apply to client-server services mapped over the *Manufacturing Message Protocol* (MMS). There are performance classes for control and protection (P1, P2, P3), metering and power quality (M1, M2, M3) and timing (T1, T2, T3, T4, T5). It is interesting to highlight that the parameter required to specify a performance class depends on what kind of traffic class we are talking about. Traffic lasses related with control and protection (P1, P2, P3) are rated by a maximum transmission delay and classes related with timing (T1, T2, T3, T4 and T5) are classified by their required time accuracy.

Regarding timing, IEC 61850-5 does not give absolute accuracy requirements for synchronization. It rather defines the requirements for the resulting time accuracy in the whole system leaving for the implementation to decide how accurate must be the timing reference to achieve the required system accuracy level. For example, the required system-wide accuracy for event time stamping (class T1) is one millisecond but it is up to the implementation to decide how good has to be the reference (GNSS, PTP...) to achieve this accuracy level. However, most of the times it is safe to assign to the timing source an accuracy one order of magnitude better than the accuracy given in the corresponding timing performance class. Following this rule, timing for event stamping would need to be at least 100 μs accurate.

11.2. MMS, GOOSE, SV

The MMS protocol has the particularity of being an ISO / IEC standard built around the 7-layer Open Systems Interconnection (OSI) model. However, it would be difficult to implement the MMS with state-of-the-art technology using only OSI protocols. Specifically, the Internet Protocol (IP) doesn't fit in the 7-layer OSI framework. The adopted solution is to split the protocol stack in Transport Profiles (T-Profiles) and Application Profiles (A-Profiles). The former covers OSI layers from 1 to 4 and the latter covers layers 5, 6 and 7. The advantage of this approach is that the OSI T-Profile can now be replaced by a TCP / IP T-Profile. The result is an hybrid protocol stack with an A-Profile made of ISO Session, Presentation and Application protocols mapped over the TCP / IP T-Profile. The glue between ISO and TCP / IP protocols is standard RFC 1006 which defines a mapping for ISO transport services on the top of TCP. IEC 61850 still provides support for a T-Profile made of ISO protocols and without support for IP but it is very hard to find real implementations based on this alternative.

GOOSE and SV have their own mappings to communications protocols. GOOSE provides a fast and reliable system-wide distribution of input and output data values.The GOOSE protocol has an specific scheme of re-transmission to achieve the appropriate level of reliability: GOOSE publishers encode and transmit GOOSE messages on multicast associations when certain events, such as the change of a data set member, are recorded. Additional reliability is achieved by re-transmitting the same data with gradually increasing retransmission time. As the publisher-subscriber approach is not well suited for bidirectional transmission, GOOSE does not require any kind of acknowledgement mechanism. It is assumed that subscribers will receive enough copies of the message to allow for a proper operation.

GOOSE messages are more simple than SSM to allow for higher transmission efficiency in terms of delay. There is no need to map GOOSE over TCP and IP and the messages could be embedded in Ethernet frames with the appropriate Ethertype. Moreover, all GOOSE packets are time stamped to allow the subscribers to check the age of the message and enable performance monitoring with its peer. GOOSE publishers require synchronization from an external timing source in order to generate accurate time stamps for GOOSE messages. Subscribers may also need external timing if they need to compare GOOSE time stamps with accurate UTC time. Today it is feasible to distribute accurate time from the substation clock using IEEE 1588v2 through the station or process bus.

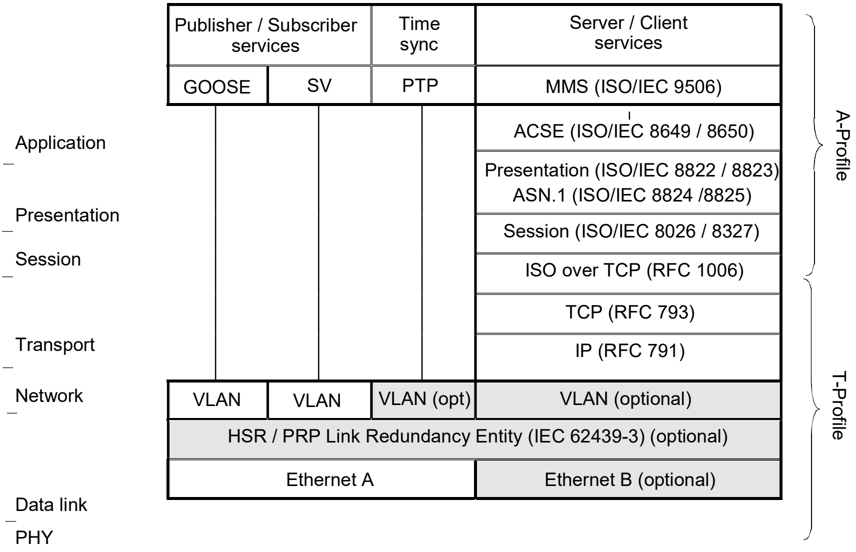


Figure 11.2: Structure of the IEC 61850 standards

The second example of peer-to-peer communications is provided by the SV protocol that implements a mechanism to distribute voltage and current samples from the power line through the process bus. To understand how the SV protocol works it is necessary to introduce the concept of Merging Unit (MU). MUs, are logical devices with the ability to collect the physical magnitudes from instrument current and voltage transformers (CTs, VTs), generate samples from these magnitudes and distribute the result of this operation in a packet switched network through an specialized protocol. MUs interactions with CTs and VTs may be based on proprietary interfaces but the distribution of sampled values is standard and, potentially, IEDs from different vendors could decode and use the information generated by any MU.

Availability of current and voltage samples is important in protection applications because protective relays must receive accurate information about the power line status. Before the introduction of IEC 61850, relays had to be cabled directly to CTs and VTs to evaluate the line status but today all that is needed is a communications

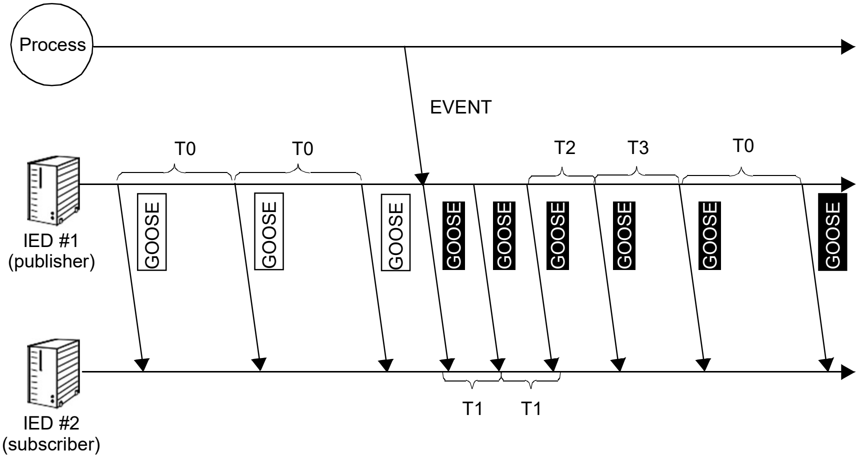


Figure 11.3: Illustration of GOOSE reliable but unacknowledged transmission.

interface that is typically an optical fibre. A multicast association is established between the MU (publisher) and one or several protection relays (subscribers).

Time stamping of SV samples is of critical importance because it enables IEDs to carry out time-coherent correlation of two or more SV flows. This is important in disturbance recording applications and differential protection schemes.

We already know that GOOSE and SV are mapped to Ethernet through a quite simple encapsulation. The standard defines which multicast addresses to use, which VLAN tags and the default priority for each protocol message. The encoding mechanism for the data structures transported over GOOSE and SV is slightly more involved and it is an application of the so called OSI Abstract Syntax Notation One (ASN.1) Basic Encoding Rules (BER), an international standard for data networks and open system interconnection.

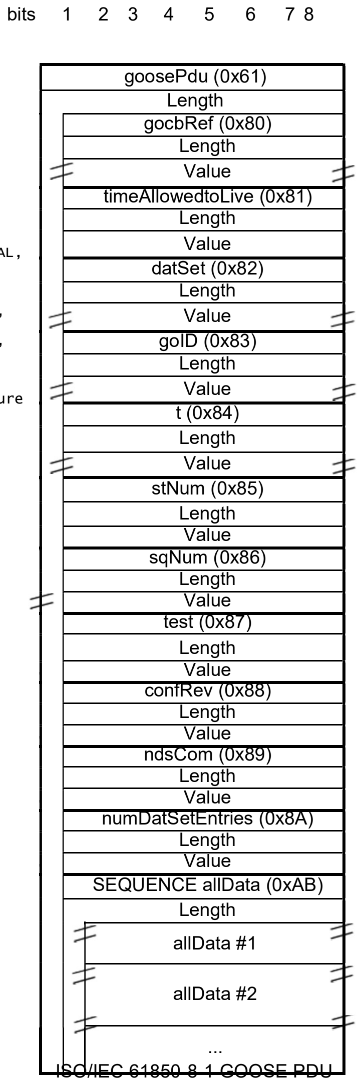
Based on the ASN.1 BER, every data component in GOOSE and SV payloads is presented in the form oa Tag-Length-Value (TLV) structure where *Tag* indicates the type of information presented by the frame, *Length* reports the length of the Value field in the form of number of bits and *Value* contains de actual encoded data. The data inside Value is consistent with the type specified by the Tag word. In adition it is allowed that Value fields could contain more TLV resulting in a tree structure.

The GOOSE message exact structure depends on the specific data to be transported. The protocol is flexible enough to accept boolean, integer, textual and other data types. Semantics are determined through the dataset (*datset* TLV) and by the GOOSE control block that manages the GOOSE flow (*gocbRef* TLV). The GOOSE message structure also contains fields that enable the subscribers to control the data flow such as the

```
IEC 61850-8-1 Specific Protocol ::= CHOICE {
   gseMngtPdu [APPLICATION 0] IMPLICIT GSEMgmtPdu,
   goosePdu     [APPLICATION 1] IMPLICIT IECGoosePdu,
   ...}



IECGoosePdu ::= SEQUENCE {
   gocbRef             [0] IMPLICIT VISIBLE-STRING,
   timeAllowedtoLive [1]  IMPLICIT  INTEGER,
   datSet              [2] IMPLICIT VISIBLE-STRING,
   goID                [3] IMPLICIT VISIBLE-STRING OPTIONAL,
   t                   [4] IMPLICIT UtcTime,
   stNum               [5] IMPLICIT INTEGER,
   sqNum               [6] IMPLICIT INTEGER,
   test                [7] IMPLICIT BOOLEAN DEFAULT FALSE,
   confRev             [8] IMPLICIT INTEGER,
   ndsCom              [9] IMPLICIT BOOLEAN DEFAULT FALSE,
   numDatSetEntries [10]  IMPLICIT  INTEGER,
   allData            [11] IMPLICIT SEQUENCE OF Data
   security           [12] ANY OPTIONAL
                           -- reserved for digital signature
```



state number (*stNum* TLV) and sequence number (*sqNum* TLV). Critically, GOOSE messages also contain a time stamp (*t* TLV). This field can be used for performance analysis of the GOOSE protocol.

The SV message, which also is encoded following the ASN.1 BER rules, may contain one or several (typically one or eight) concatenaded measurements from the merging unit. Each of measurements is made up ofseveral samples. In a three-phase system

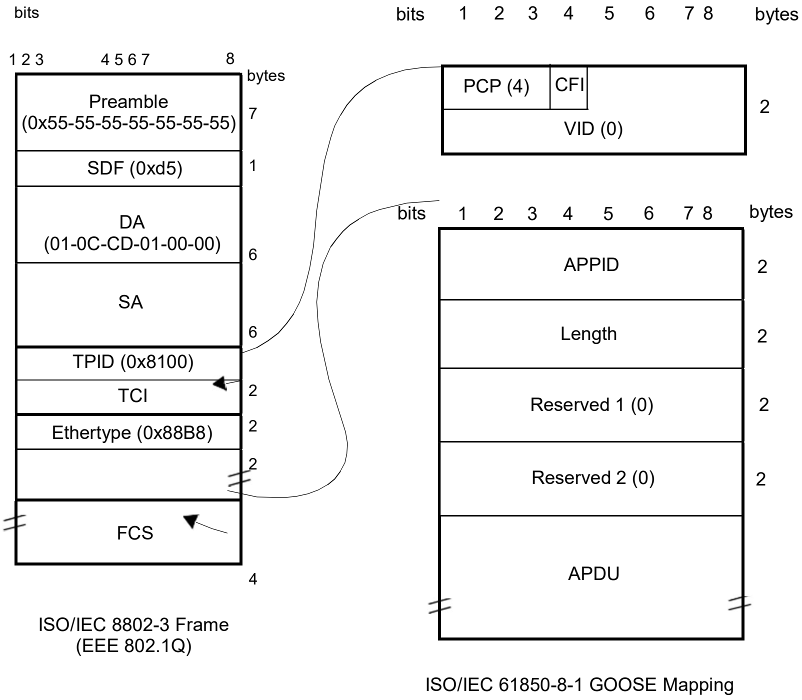


Figure 11.4: GOOSE mapping to Ethernet (IEEE 802.3Q) frames.

the measurement result has eight samples (four currents, 3 phases plus ground values and four voltages also from the three phases and ground). Voltage and current samples are formatted with the data structure defined by IEC 81850-7-3 specifically for this purpose. This data structure has support not only for the numeric value of the measured current or voltage but it also provides information about validity and quality of the measured value. It can also optionally provide a time stamp but it is more common that the SV data flow is synchronized by means the *smpCnt* field included in each concatenaded measurement from the SV message. If the merging unit is externally synchronized by a pulse mechanism (1PPS, for example) the *smpCnt* field is reset to zero with every timing pulse. This mecanism enables accurate time alignment of sampled data by just looking at one field in the sampled value measurement result.

11.3. GOOSE and SV Protocol Timing Analysis

We have seen that timing is an essential feature for GOOSE and SV applications and for this reason GOOSE messages are time stamped and SV data flows include a mechanism that enables metering and protection nodes such as relays to combine and align data from different sources. Tempo decodes the IEC 61850 protocols and runs a detailed analysis of the embedded timing to verify its validity. In GOOSE applications

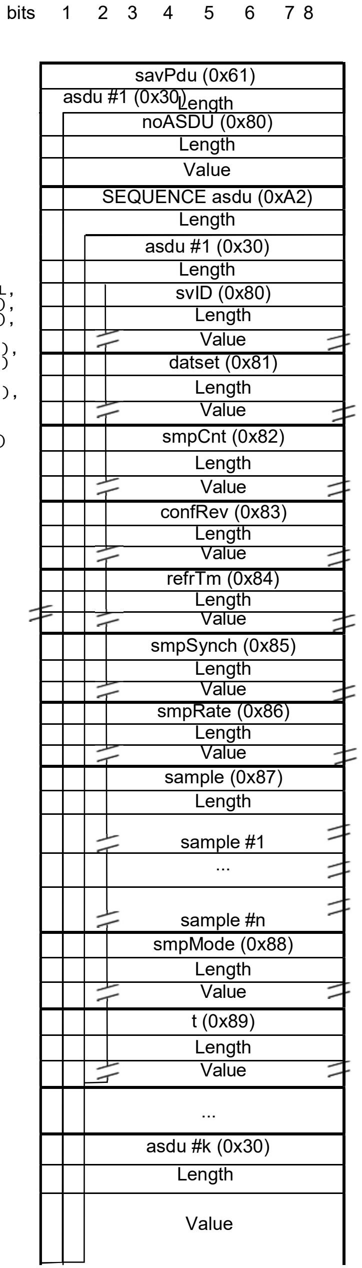
```
IEC 61850-9-2 Specific Protocol ::= CHOICE {
    savPdu [APPLICATION 0] IMPLICIT SavPdu,
    ...}



SavPdu ::= SEQUENCE {
    noASDU              [0] IMPLICIT INTEGER (1..65535),
    SECURITY            [1] ANY OPTIONAL,
    asdu                [2] IMPLICIT SEQUENCE OF ASDU,
    }

ASDU ::= SEQUENCE {
    svID                [0] IMPLICIT VisibleString
    datset              [1] IMPLICIT VisibleString OPTIONAL,
    smpCnt              [2] IMPLICIT OCTET STRING (SIZE(2)),
    confRev             [3] IMPrICIT OCTET STRING (SIZE(4)),
    refrTm              [4] IMPLICIT UtcTime OPTIONAL,
    smpSynch            [5] IMPLICIT OCTET STRING (SIZE(1)),
    smpRate             [6] IMPLICIT OCTET STRING (SIZE(2))
                            OPTIONAL,
    sample              [7] IMPLICIT OCTET STRING (SIZE(n)),


    smpMode             [8] IMPLICIT OCTET STRING (SIZE(2))
                            OPTIONAL,
    t                   [9] IMPLICIT UtcTime OPTIONAL,
    }
```



ISO/IEC 61850-9-2 SV PDU

Tempo compares the GOOSE time stamps with locally generated timing marks providing information about the validity and performance level of these time stamps. In SV applications the timing analysis is related with 1PPS tests: The analyser checks the *smpCnt* field in the first measurement carried in the SV message and computes the time offset between samples carrying a zero smpCnt and locally generated time stamps.

11.3.1. GOOSE and SV Test Configuration

The GOOSE and SV timing tests require that the unit is previously disciplined by an external time synchronization source. The alternatives are ToD, IRIG-B and GNSS (See section 2.6). Once the clock reference is ready, this is the procedure to configure the test:

1. Make sure that your tester is connected to the network. The physical layer must be up and working (See section 4.1.1).
2. From the *Home* panel, go to *CONFIG*,
   The port setup panel is displayed.
3. Choose between *Ethernet endpoint* or *IP endpoint* with the *Mode* setting.
4. From the *Home* panel, go to *TEST*,
   The test configuration panel is displayed.
5. Go to Protocol analysis.
6. Choose between *GOOSE* or *Sampled Values* depending of the protocol you wish to monitor.
   Note: It is also possible to enable *GOOSE* and *Sampled Values* analysis at the same time.
7. Enable the analysis by configuring *Enable* to *On*.
   Note: Enabling GOOSE or Sampled Values analysis modifies the filter configuration by forcing a *GOOSE* filter in stream A1 and / or a *SV* filter in stream A2. This setting is not reverted when the GOOSE / Sampled Values analysis is disabled and if a different configuration is required, it has to be modified by hand (See section 6.2).
8. Optionally, enable *Application ID match* to run the analysis only in frames with an specific value of the *Application ID* field.
9. If you have enabled the Application ID filter in the previous step configure the value of the *Application ID* to be considered by the analysis.
10. Optionally, configure *Filter / Discovery by field* to *GoCBRef*, *GoID* or *DatSet* (GOOSE analysis) or to *SvID* (Sampled Values analysis) to refine even ore the analysis by considering only frames with certain custom properties.
11. Configure the value of the filter / discovery field in accordance with the settings from the previous step or let the unit choose the value with the help of the discovery mechanism described below in this section.

In some testing scenarios it may be difficult to know in advance the value of the GOOSE or SV field to be used for analysis. Then it may be useful to scan the network to retrieve information about active flows identified by their data of interest. This is a function that Tempo could provide by following these steps:

1. Make sure that the Filter / Discovery by field from the Sampled Values or GOOSE protocol analysis configuration screens is configured to anything different to *Any*.
2. Go to Discovery.
3. Press the Start contextual button.
   The SV Discovery or GOOSE Discovery table is populated with the available traffic flows detected in the network and identified by their *GoCBRef*, *GoID*, *DatSet* or *SvID* depending on the settings of *Filter / Discovery by field.*
4. Press the Stop contextual button.
   The discovery process stops.
5. Select the item in the list you wish to use in the protocol analysis with the help of the check box.

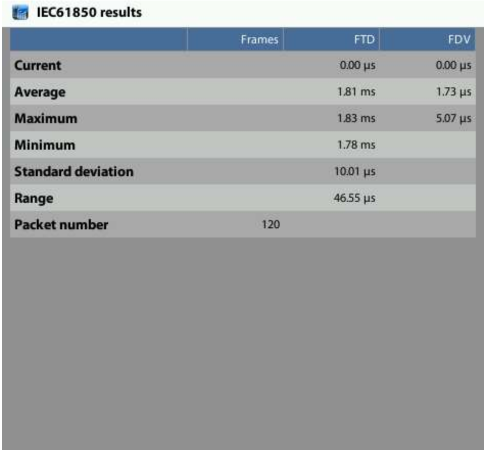
11.3.2. Running the GOOSE / SV Test

Once the test has been configured following the procedure described in the previous section the test could be started at any point by pressing the run key. This is the correct procedure to display the recorded GOOSE and Sampled values results:

Table 11.1: IEC61850 Delay Results

Field	Description
Frames	Counts the number of frames matching with the analysis filters received from the beginning of the test. These are the total amount of frames used in the latency analysis.
FTD	Value of the point-to-point GOOSE or Sampled values Ethernet *Frame Transfer Delay* (FTD) computed as specified in ITU-T Y.1563 and expressed in time units. The tester provides different statistics based on the FTD: *Current* value, *Average*, *Maximum*, *Minimum*, *Standard deviation* and *Range*. To display the current FTD it is required a previous initialization of a test with *Run*.
FDV	Reports the jitter computed as per RFC 3393 and RFC 1889. The *Frame Delay Variation* (FDV) is computed over consecutively transmitted packets. The current jitter value is smoothed with the function defined in RFC 1889 before being displayed. The unit reports not only the current FDV but also the Average and Maximum values too. To display the jitter statistics it is required a previous initialization of a test with *run*.

1. From the *Home* panel, go to *RESULTS*,
   The test port results panel is displayed.
2. Select either *Port A or Port B* to enter in the port specific results.
3. Go to *GOOSE Results or SV Results.*
4. Check de *Frames*, *FTD* and *FDV* statistics.



IEC61850 results

	Frames	FTD	FDV
Current		0.00 µs	0.00 µs
Average		1.81 ms	1.73 µs
Maximum		1.83 ms	5.07 µs
Minimum		1.78 ms	
Standard deviation		10.01 µs	
Range		46.55 µs	
Packet number	120		

Figure 11.5: GOOSE mapping to Ethernet (IEEE 802.3Q) frames.

Chapter 12
Test Management

This chapter describes all those features available in your test unit that are not directly related with configuring your tester or reading measurement results but they are important for proper test management. Specifically, configuration and result management, report generation and test platform settings are covered in the following sections.

12.1. Generating Reports

Users may want to generate reports based on their measurements. Reports are important to save results for later reference. Reports can be used to share a test result or to include results in documents.

Depending on the purpose of the report, users have different ways to generate and store them. The test unit offers maximum flexibility and at the same time simplicity when configuring reports. Follow these steps to configure and generate a report:

1. From the *Home* panel, go to *File* (🗋),
   The tester file manager base menu is displayed.
2. Select *Report files* to go to the report file settings
3. Enable report generation by means the *Generate reports* control.
4. Set the *Report format*, *Report named after* and *Report header* fields.
5. If you have set *Report named after* to *User ref.+sequence*, configure the *User reference* field to the desired sequence.
6. Optionally, if you have configured *Report named after* to *User ref.+sequence* or *Serial no.+sequence*, enter the *Next sequence number* to be applied to the next report.
7. Set the correct action to be carried out when the internal storage is full.

If report generation is enabled, a new report is generated each time a test finishes either by pressing the run button or automatically. Reports are available as standard text or PDF files from the USB slave connector and they can be exported through the USB master port, the SD card reader or the web interface.

Table 12.1: Report Files Panel

Setting	Description
Internal memory	Displays report files stored in the internal tester memory. The test unit stores up to 50 report files.
External devices	Displays report files stored in external devices (micro SD memory card, USB memories or drives) connected to the tester. The amount of files stored in an external device is only limited by the device capacity.
Generate reports	Enables / Disables report generation.
Report format	Selects the report format for future reports. • *PDF*: Reports are generated using the portable document format (PDF). Use this configuration if you want to make difficult for anyone to modify the report. • *Plain text*: Reports are text documents which can be edited with any text editor. Use this configuration if you want to modify the report or include it in a wider document.
Report named after	This control enables the user to choose between different templates for the report name. There are three different templates to choose: • *Start time*: The report is identified by a time stamp that contains both data and time with the following format: yyyy-MM-dd-hhmmss. • *User ref. + sequence*: The report name is set to a user configurable string plus a sequence number that is incremented for each new test. • *Serial no. + sequence*: The report name is set to the tester serial number plus a sequence number that is incremented for each new test.
User reference	This could be any alphanumeric string containing upper case letters, lower case letters and numeric digits. This field makes sense only if the report name format is *User ref. + sequence*.
Next sequence	Displays and configures the sequence number that will be assigned to the next report to be generated. This field makes sense only if the report name format is *User ref. + sequence* or *Serial no. + sequence*.

Table 12.1: Report Files Panel

Setting	Description
Report header	This menu item enables you to configure report data that will be stored with the test result. These data identify the report, customer, and also includes some other relevant information. • *Customer*: Field that can be used to set the company where the test report applies. • *Department*: This field can be used to identify the department where the user that has carried out the tester. belongs. • *Company*: This is the field that identifies the company that carries out the test. • *Location*: This describes where the test results from the network were recorded. • *Operator*: This field may contain the name of the operator that owns the network infrastructure where the test was run.

12.2. Taking Screenshots

Sometimes it is convenient to have a simple procedure to store an specific setting, result or plot. Tempo is able to generate screenshots with this purpose. To generate an screenshot just touch at the “photo camera” icon on the top of the screen. Screenshot files are stored in PNG format and they can be renamed, deleted and exported from the unit using the file manager (See section 12.3).

12.3. File Management

Tempo stores configurations, screenshots, event logs and reports in files. These files can be deleted, renamed or exported to an external USB memory or micro SD card. Configurations can be shared between different test units by means compatible storage devices. Report files can be included to documents, sent by e-mail or printed. Event logger files can be processed by external software packages to generate sophisticated plots or other kinds of data representations.

12.3.1. Saving Configurations

To store the current configuration follow these steps:

1. From the *Home* panel, go to *File* (🗋),
   The tester file manager base menu is displayed.
2. Select *Configuration files* to go to the configuration file settings.

3. Select the location to save the configuration: *Internal memory*, or *External devices*.
   Note: If you select E*xternal devices*, you will be asked to choose the specific storage device (USB device or micro SD card).
   Note: If there is no external device connected to the unit, a *No devices present* popup panel is displayed.
4. Press the *Save* contextual button.
5. Enter a file name for the configuration file that is going to be saved and confirm with the *Done* contextual button.

12.3.2. Renaming Files

Configurations, screenshot files, event logger files and report files can be renamed after they are created. To rename files follow these sequence:

1. From the *Home* panel, go to *File* (🗋),
   The tester file manager base menu is displayed.
2. Select *Configuration files*, *Event logger files, Report files* or *Screenshot files*.
3. For *Configuration files* and *Report files*, select the location of the file you want to rename: *Internal memory*, or *External devices*.
   Note: If you select E*xternal devices*, you will be asked to choose the specific storage device (USB device or micro SD card).
   Note: If there is no external device connected to the unit, a *No devices present* popup panel is displayed.
4. Select the file you want to rename.
   Note: You can select several files in the list, but renaming of many files at the same time is not allowed.
5. Press the *Rename* contextual button.
6. Enter the new file name for the selected configuration or report file with the alphanumeric keyboard. Confirm with the *Done* contextual button.

12.3.3. Deleting Files

With the file manager you can delete files that are not needed anymore. To do that follow these steps:

1. From the *Home* panel, go to *File* (🗋),
   The tester file manager base menu is displayed.
2. Select *Configuration files, Event logger files, Report files* or *Screenshot files*.
3. Select the location of the file you want to delete: *Internal memory*, or *External devices*.
   Note: If you select E*xternal devices*, you will be asked to choose the specific storage device (USB device or micro SD card).
   Note: If there is no external device connected to the unit, a *No devices present* popup panel is displayed.

4. Select the file you want to delete.
   Note: You can select several files in the list at the same time.
5. Press the *Delete* contextual button.
6. Enter the new file name for the selected configuration or report file with the alphanumeric keyboard. Confirm with the *Done* contextual button.

12.3.4. Exporting Files to External Devices

Configuration files, report files, event logs and screenshot files can be exported to external devices like USB memories or micro SD cards. The procedure is as follows:

1. From the *Home* panel, go to *File* (🗋),
   The tester file manager base menu is displayed.
2. Select *Configuration files*, *Report files, Event logger files* or *Screenshot files*.
3. Select *Internal memory*, to list the files currently stored in the unit.
4. Select the files you want to export.
5. Press the *Export* contextual button.
   A popup menu to select the external device where the files will be exported is opened.
   Note: If there is no external device connected to the unit, a *No devices present* popup panel is displayed.
6. Select an external device, confirm, and wait for the files to be copied.

Remove the USB storage device or micro SD card from the unit.

12.3.5. Importing Configurations

If you have a configuration file from a compatible tester you can import and load this file in your unit to reproduce similar measurements. This is the procedure you have to follow:

1. From the *Home* panel, go to *File* (🗋),
   The tester file manager base menu is displayed.
2. Select *Configuration files* to go to the configuration file settings.
3. Select *External devices* to list the files currently stored in the external device.
   A popup menu to select the source external device is opened.
   Note: If there is no external device connected to the unit, a *No devices present* popup panel is displayed.
4. Select the configuration files you want to import.
5. Press the *Import* contextual button, confirm, and wait for the files to be copied from the internal memory.
6. Remove the USB storage device or micro SD card from the unit.

12.3.6. Verifying the Current Disk Usage

Configurations, *Reports* and *Event logs* share the same storage space in the disk. Users are allowed to check which is the disk occupation status and depending on the result they can decide to delete files of a certain type. The procedure to do that is as follows:

1. From the *Home* panel, go to *File* (🗋),
   The tester file manager base menu is displayed.
2. Select *Disk usage*.
   The disk usage is displayed graphically and the storage space used for each file type is shown in KB or MB.
3. Optionally, select *Configuration files*, *Report files* or *Event logger files* and delete all files of these type with the appropriate contextual key.

12.3.7. Configuring What to Do When the Disk is Full

Users decide what to do when the disk storage capacity is exhausted. The available options are:

- *Block measurements*: No new measurements can be run when the internal memory is full.
- *Stop file generation*: New measurements are run even if the internal memory is full but no reports are generated for them.
- *Delete oldest files*: When the maximum available capacity is reached, new files replace the older ones. Use this action with care. No warning is displayed when old reports are deleted.

To configure this action, the correct procedure is:

1. From the *Home* panel, go to *File* (🗋),
   The tester file manager base menu is displayed.
2. Configure *Action when disk full* to *Block measurements*, *Stop file generation*, *Delete oldest files*.

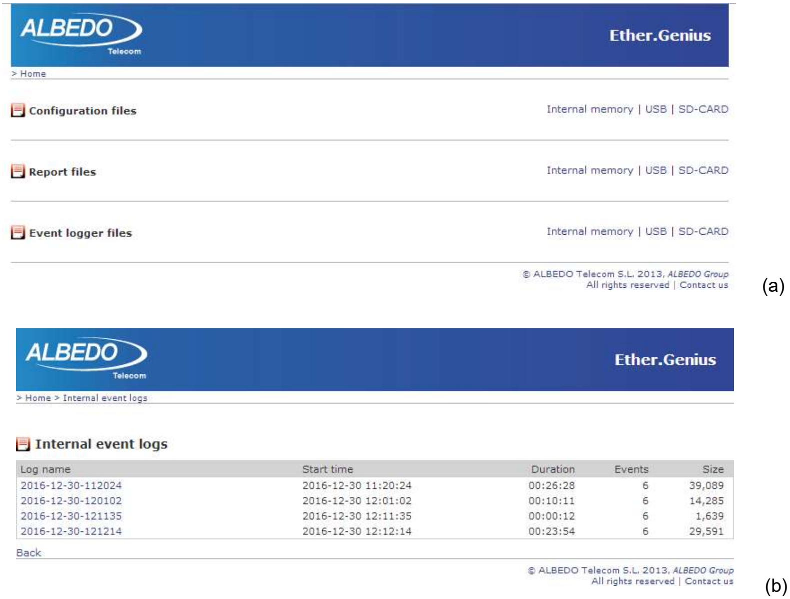
12.3.8. Using the EmbeddedWeb Server

As an alternative of using a USB external storage device or a micro SD card for file management, the tester has a web interface that can be used for the same purpose.

The web interface can be used for downloading configurations, reports and event log files from a remote computer without using any accessory other than an standard network connection. Currently, the web interface does not support file uploading but for this purpose, the USB and micro SD interfaces are still available.

To use the web interface you need to connect the platform network connector to the management network and configure the management Ethernet interface (See section 12.5.1). Once you have done this, follow this procedure:

1. Open a browser in a computer with network connection.
2. Type the IP address you have assigned to the tester in the browser destination URL.
   The web interface home panel is displayed in the Internet browser.
3. Choose the files you want to display (*Configuration flies*, *Report files, Event logger files* or any other if available) and the location of these files (*Internal memory*, *USB*, *SD-CARD*) and press to the correct hyper link.
   A list with the available files for the selected category is displayed in the web browser.
4. Select the file you want to download it to the local computer.
   The web browser displays a dialogue that requests your configuration to download the selected file. If you accept, the file will be downloaded.



ALBEDO Telecom

Ether.Genius

> Home

Configuration files — Internal memory | USB | SD-CARD

Report files — Internal memory | USB | SD-CARD

Event logger files — Internal memory | USB | SD-CARD

© ALBEDO Telecom S.L. 2013, *ALBEDO Group*
All rights reserved | Contact us

(a)

ALBEDO Telecom

Ether.Genius

> Home > Internal event logs

Internal event logs

Log name	Start time	Duration	Events	Size
2016-12-30-112024	2016-12-30 11:20:24	00:26:28	6	39,089
2016-12-30-120102	2016-12-30 12:01:02	00:10:11	6	14,285
2016-12-30-121135	2016-12-30 12:11:35	00:00:12	6	1,639
2016-12-30-121214	2016-12-30 12:12:14	00:23:54	6	29,591

Back

© ALBEDO Telecom S.L. 2013, *ALBEDO Group*
All rights reserved | Contact us

(b)

Figure 12.1: Tempo web interface: (a) Home panel (b) Event logger file management panel.

12.4. Programming Tests

Tempo is able to start and finish tests without direct user intervention. All automatic testing features are included within the *Autostart/stop* menu.

Follow these steps to program an automatic measurement in the test unit.

1. From the *Home* panel, go to *TEST*,
   The test configuration panel is displayed.
2. Select *Autostart/stop* to enter in the automatic test programming menu.
3. If you want the automatic test to start at a specific date and time set *Start mode* to *Auto* and enter the start date and time in *Start time.*
   Note: Manual start has precedence over auto-start. That means that if a tester is started by pressing *Run* but there is an automatic test programmed the manual test will start anyway.
4. If you want the automatic test to stop at a specific time after it has started set *Stop mode* to *Auto* and enter test duration with the help of the *Duration* and *User duration* controls*.*
   Note: Manual stop has precedence over autostop. That means that if a tester is stopped by pressing *Run* but there is an automatic test programmed the manual test will stop anyway.

Table 12.2: Autostart / stop Panel

Setting	Description
Start mode	Configures the start test mode. There are two different choices here: • *Manual*: The test starts when there is not an ongoing test and *Run* is pressed. • *Auto*: The test starts at a configured date and time without the need of pressing any key.
Start time	Enter the start date and time for the next automatic measurement with the following format: *dd/MM/yyyy hh:mm:ss*. To configure Start time, you have to set *Start* mode to *Auto* before.
Stop mode	Configures the stop test mode. There are two possibilities: • *Manual*: The test finishes when there is an ongoing test and *Run* is pressed. • *Auto*: The test finishes when a configurable test duration is reached. This mode does not require user intervention once the duration has been set and the measurement has started.
Duration	Sets the duration of the next measurement. The available test durations are: 15 minutes, 1 hour, 1 day, 7 days, 30 days or user configurable duration. Setting up *Duration* requires previous configuration of *Stop Mode* to *Auto*.

Table 12.2: Autostart / stop Panel

Setting	Description
User duration	Sets the duration of the next measurement when *Stop mode* has been configured to *Auto* and *Duration* to *User*. The duration has to be entered in a *hh:mm:ss* format.
Last started on	Displays the date and time when the last measurement was started.
Last stopped on	Displays the date and time when the last measurement was stopped. If there is an ongoing test, the value of this field is empty.
Last power down on	Displays the date and time when the tester waspowered down for last time.

12.5. Using the System Menu

The System menu includes platform wide settings organized in four different sub-menus:

- *General settings*: This menu includes controls to manage the way the user interface behaves and how the information is presented.
- *Network configuration*: Includes the IP configuration corresponding with the platform NIC.
- *System information*: This menu has the test unit model name and serial number and software, firmware and hardware versions.
- *Licensing*: This is a menu that displays the software versions installed in the tester and enables their management.

Table 12.3: General Settings Panel

Setting	Description
Brightness (%)	Sets the screen brightness from 10% to 100%. Within the *Brightness* panel, the left and right cursors are used to set the correct value and a contextual key (*Done*) is used to confirm selection.
Keyclick	Enables or disables the keyclick. The keyclick is a sound that is played each time a key is pressed.
Language	Selects the user interface language. Menus, selection lists and results are presented in the language selected here. The languages currently available are English and Spanish.

Table 12.3: General Settings Panel

Setting	Description
Clock setup	Configures the system time and date. You can either type the correct date and time manually or let the equipment to retrieve the correct values from a *Network Time Protocol* (NTP) server.
Time display	Select the way the time is displayed in the graphical user interface. One of the following has to be selected: • *Elapsed*: Time from the beginning of the test is displayed with the following format *hh:mm:ss*. If there is not an ongoing test, then the duration of the last test is shown • *Absolute*: The current date and time is displayed with the following format: *dd/MM/yyyy hh:mm:ss*.
Screensaver	Sets or unsets the screen saver. The screen saver reduces power consumption and increases operation time under battery operation.
Screensaver delay	Configures the delay to switch the screensaver on. The backlight brightness is set to a low value once the time configured here has finished. The display backlight is switched off after twice the screensaver delay. The available configuration values for this item are: 10s, 30s, 1min, 2min, 5min, 10min, 20min.
Remote control	This is a menu that contains the controls necessary to enable and configure the VNC remote control. The items contained in this menu are: • *Enable*: Enables or disables the Ethernet / IP remote control. The remote control is an optional feature that enables remote users to use the tester from a computer running VNC. • *Remote control password*: Configures a password for the remote control. Any alphanumeric string should be accepted. Use the same password in the remote VNC client to access to the tester user interface.

Table 12.3: General Settings Panel

Setting	Description
SNMP	This menu contains the controls necessary to enable and configure SNMP in units compatible with this protocol. The items contained in this menu are: • *Enable*: Enables or disables the SNMP server in the unit. If this setting is configured to *On*, the SNMP server is enabled and it responds to SNMP requests. If *Enable* is configured to *Off*, then the unit ignores SNMP requests. • *Read community*: Community name used for read operations. Write operations based on the read community name will fail. The default read community is *public*. • *Write community*: Community name used for write operations. The write community can be used for read operations as well. The default write community is *private*.

There is also a *Reset to factory defaults* control in the system menu that enables to recover de default configuration in the test unit. Please, note that the settings from the System menu, including network settings, clock settings and others, are not restored with this control.

This section supplies a description of the *General settings* menu and *System information* menu. To learn how to configure and use the network interface or how to install licenses for new software options go to the sections specifically dedicated to these topics.

Table 12.4: System information panel

Setting	Description
Model Name	Shows the test unit model name: Tempo.
Serial number	Displays the test unit serial number. It is a 8 character alphanumeric string
Software version	Displays the current software release.
Hardware version	Displays the current hardware release.
PM release	Displays the current power management release.
Firmware versions	Displays the current firmware release.

12.5.1. Using the Network

The platform network interfaces are currently user for three different purposes:

- *IP remote control*. This feature enables any user to access to the equipment from a remote location, configure a test, run it and display the results.
- The *Web interface*: This is used to retrieve reports configurations or any other file available in the tester internal memory or attached storage device.
- *Maintenance and factory configuration*: The Calnex staff use the plat- form network interfaces to configure or verify the equipment in the factory. This feature is not available to ordinary users.

Table 12.5: Network Configuration Panel

Setting	Description
Ethernet interface	Configuration menu for the platform network interface. This menu can be used to configure the interface IP address and mask either automatically (DHCP) or statically.
Wireless interface	Configuration menu for the platform wireless network interface. This menu is used to set the radio parameters for the interface such as the SSID and the network parameters like the IP address and mask. The wireless interface requires a compatible WiFi adapter for the USB port. This adapter is supplied by Calnex as an optional accessory.

Before you can use the network interface you need to enable the interface and configure an IP profile either automatically through DHCP or by hand. If you are using a wireless interface you also need to enter the radio interface and encryption settings.

Table 12.6: Network Interface Configuration

Setting	Description
Enable interface	Enables or disables the network interface. Note that the link led placed in the Ethernet platform connector is lit even if the interface is not enabled.
Wireless network	This is a menu that configures the WiFi in wireless interfaces. It contains settings such as the ESSID or the wireless encryption protocol. This menu is not available in Ethernet interfaces.

Table 12.6: Network Interface Configuration

Setting	Description
Use DHCP	Configures the mechanism used to set the interface IP address and mask (and also other system-wide settings like the gateway address and the DNS server). If *Use DHCP* is enabled, the IP profile is configured automatically using a DHCP server installed in the network. Otherwise, the user has to enter the IP address, mask, default gateway and DNS address by hand.
Static IP address	Static IP address assigned to the interface in a decimal four dotted format. This setting makes sense only if *Use DHCP* is not enabled.
Static network mask	Static network mask in a decimal four dotted format. This setting makes sense only if *Use DHCP* is not enabled.
Fixed gateway address	IP address corresponding to the network device used to send IP packets to external networks. The gateway address is configured in decimal, four-dotted format.
Fixed DNS address	IP address corresponding to the host used for domain name resolution. A DNS server allows the user to identify destinations by alphanumeric domain names rather than numeric IP addresses. The DNS address has to be entered in decimal, four-dotted format.
Leased IP address	Current DHCP-assigned IP address in a decimal four dotted format. This is a read-only field that cannot be directly configured by users This setting makes sense only if *Use DHCP* is enabled.
Leased network mask	Current DHCP-assigned network mask in a decimal four dotted format. This is a read-only field that cannot be directly configured by users. This setting makes sense only if *Use DHCP* is enabled.
Leased gateway address	Current DHCP-assigned default gateway in a decimal four dotted format. This is a read-only field that cannot be directly configured by users This setting makes sense only if *Use DHCP* is enabled.
Leased DNS address	Current DHCP-assigned DNS server in a decimal four dotted format. This is a read-only field that cannot be directly configured by users This setting makes sense only if *Use DHCP* is enabled.

Table 12.6: Network Interface Configuration

Setting	Description
Ethernet address	48-bit physical address of the NIC attached to the test unit. In Ethernet interfaces, this address is assigned to the NIC when it is manufactured and it cannot be changed later. In wireless interfaces, the Ethernet address corresponds with the MAC address assigned to the external WiFi adapter by the manufacturer. Replacing the adapter modifies the MAC address.

To configure and use the platform network interfaces follow these steps:

1. If you are using an Ethernet interface, connect the platform Ethernet connector (platform panel, RJ-45 connector with the *Ethernet* label) to the management network. If you are using a wireless interface, attach a compatible USB dongle to the platform USB connector (USB master connector in the platform connector panel).
2. From the *Home* panel, go to *System*,
   The general system menu is displayed in the screen.
3. Select *Network configuration* to display the network configuration and management menu.
4. Go to the *Ethernet interface* or *Wireless interface*, depending on the physical medium you want to use to control de unit.
   Note: The wireless interface configuration is not available if you do not attach a compatible wireless USB dongle to the test unit USB port.
5. Enable the platform network interface with the *Enable interface* control.
6. Enable DHCP with the *Use DHCP* control if you want to let DHCP to configure your IP settings automatically or disable it to configure an static IP profile.
7. If you are not using DHCP, enter correct values for the *Static IP address*, *Static network mask*, *Fixed gateway address* and *Fixed DNS address*.
8. If you are configuring a wireless interface, go to *Wireless network* and configure the *Association mode*, *ESSID network*, *Encryption* and *Type of key*. Depending on the *Type of key* configure the *Hexadecimal key*, *ASCII key* and *Key number*.
9. Optionally, check from a remote computer that the equipment is responding to ping requests.

If you are configuring a wireless interfaces there is an specific configuration to be done before you can set the IP layer. These configuration includes the setting of the wireless network

Table 12.7: Wireless interface settings

Setting	Description
Association mode	Configures the way the test unit has to access to communicate to other devices through the wireless interface: There are two different possibilities: • *Infrastructure*: The unit is connected to a central point known as wireless access point. The access point bridges traffic to the wired network or to other wireless devices but there is never a direct communication between two wireless end points. • *Ad-Hoc*: There is a direct association between two wireless end points without the mediation of any access point.
ESSID network	Extended Service Set Identification. In a infrastructure wireless network it identifies the access point where the endpoints are connected. In ad-hoc connections there is no access point but the ESSID still operates as a network identifier. The ESSID has to be the same in ad-hoc communicating peers.
Encryption	Enables or disables encryption over the wireless interface, The encryption protocol configured in this field must match the configuration in the remote device or in the access point. The encryption schemes currently supported are WEP-64 and WEP-128. These are the details: • *Off*: Disables all encryption over • *WEP-64*: First version of the Wired Equivalent Privacy (WEP) protocol based on a 40-bit key plus a 24-bit initialization vector. • *WEP-128*; Enhanced version of the Wired Equivalent Privacy (WEP) protocol based on a 104-bit key followed by a 24-bit initialization vector

Table 12.7: Wireless interface settings

Setting	Description
Type of key	Configures the way the key for the WEP encryption is going to be entered. There are the possible configurations for this setting: • *HEX*: Configures the WEP key in hexadecimal format. For WEP-64 you have to enter exactly 10 hexadecimal digits (from 0 to 9 or *A*, *B*, *C*, *D*, *E* and *F* letters). If you are using WEP-128 you need to enter 26 hexadecimal digits. • *Passphrase*: Generates the WEP key from an alphanumeric pattern made up of upper and lower case letters, decimal digits and spaces. Specifically, the passphrase procedure could be used to generate four differentWEP-64 keys or one WEP-128 key. • *ASCII*: Configures the WEP key in ASCII format. For WEP-64 you have to enter 5 ASCII characters. If you are using WEP-128 you have to enter a 13 character key.
Hexadecimal key	Configures the WEP key in hexadecimal format (valid if *Type of key* has been configured to *HEX*). If *Encryption* is *WEP-64* the hexadecimal key is made up of 10 hexadecimal digits. If *Encryption* has been set to *WEP-128*, then you are required to enter 26 hexadecimal digits.
ASCII key	If *Type of key* has been configured to ASCII, it configures the WEP key in ASCII format. If the encryption protocol is WEP-64, the ASCII key is made up of exactly 5 characters (upper and lower case letters, decimal numbers). If you are using WEP-128 you have to enter a 13 character key. If T*ype of key* is *Passphrase*, it configures the WEP key through a variable length alphanumeric sentence which can be made of several words separated by spaces.
Key number	If you are configuring the WEP-64 protocol key through a passphrase you will be asked to supply the key number. The reason is that the passphrase procedure generates four different keys. The user has to choose the key to be used for authentication. If you are using WEP-128 then the passphrase generates only a single key and there no need to do any selection.

Table 12.7: Wireless interface settings

Setting	Description
Current key (Hex)	Displays the current key in hexadecimal format. If you have configured an hexadecimal key, the *Current key (Hex)* and the *Hexadecimal key* fields should be displaying the same but if you are using an ASCII key or a passphrase the key will not match the value you have entered.
Associated	Could be either *Yes* or *No*, depending whether the unit is associated with an access point or not. The association status does not guarantee by itself that the test unit is allowed to exchange information with the access point. Specifically, the association is still established even if the encryption standard or the key are incorrect. Associations between endpoints and access points make sense only if the *Association mode* is *Infrastructure*.

12.5.2. Installing Software Options

New software for Tempo can be licensed after the unit as been purchased when new testing needs arise. To install new software options for your unit follow this procedure.

Table 12.8: Licensing

Setting	Description
Licensed options	Shows a list with all the software options currently available in your test unit.
License key	Hexadecimal number provided by Calnex that enables secure management of the software options installed in your test unit. Enter the license key in this field before adding the new software options to your test unit.
Action	Set this field to Activate to add new software options to your tester. You have to enter the *License key* before adding new options.
Status	Displays the result of the software option activation operation performed by enabling the *Activate* field.

1. Contact with your local sales representative to purchase software options for your test units.

You will receive one variable length license key for each tester you want to upgrade.

2. From the *Home* panel, go to *System (*)*,
   The system configuration panel is displayed.
3. Select *Licensing* to enter in the software upgrade menu.
4. Enter the key supplied by your Calnex representative in *License key*.
5. Enable the new software options with the *Action* control.
6. Check that the upgrade has been successful with the help of the *Status* control.

12.5.3. Upgrading the Power Management

The *Power Management* monitors and controls the battery charge and discharge processes. This component does not change when the software and firmware are upgraded and usually remains without modification for the whole test unit live cycle. However, the Power Management runs a algorithm that users can upgrade if necessary. The procedure to do that is described below:

1. From the Home panel, go to *System* (***).
2. Open the Licensing menu.
3. Enter the maintenance password for your unit in *Service password*.
   Note: This password is different for each unit and it is supplied by Calnex Telecom on demand.
4. Press the back key to display the *System* panel again.
5. Go to *Service*.
6. Open *PM firmware update*.
7. Press the green *Update* button
   The following text is displayed: *PRESS and HOLD the reset button on the rear panel and then press the CONTINUE button at the same time*.
8. Now press the *Hardware reset* button (See section 1.2.1) and then, without releasing, press *CONTINUE*. You can also cancel the operation with *CANCEL*.
9. If you have pressed *CONTINUE* in the previous step, the power management version will be upgraded in the unit. The process takes 2 or 3 seconds.
   Once finished, the following message is displayed in the screen: *The unit will be powered off*.
10. Press CONTINUE.
    The unit is powered off.
11. Power the unit on.
12. From the *Home* panel, go to *System (*)*.
13. Open the *System information* menu.
14. Make sure that the power management button is now up to date.
15. Leave the *System information* menu with the help of the back key.
16. Go to the *Licensing* menu.

17. Delete the service password you have entered previously.

12.5.4. Using NTP and GPS/NMEA for System Clock Synchronization

The system clock controls the date and time assigned to configuration and report files and controls the auto-start / stop function. Tempo users can manually set the system time and date by entering the correct values but they can also synchronize the clock with an external NTP server or GNSS. The NTP server must be available through the management Ethernet port. The GNSS timing is received through the built in.GNSS module, if available (See section 2.6).

Table 12.9: Time Source Configuration Options

Setting	Description
Date	This is used to configure the current date. The date is used for the *Autostart/stop* features and other purposes. The date has to be entered with the following format: *dd/MM/yyyy*. You can only modify the date if the current time source has been set to *Manual*.
Time	This is used to configure the current time. The time is used for the *Autostart/stop* features and other purposes. The time has to be entered with the following format: *hh:mm:ss*. You can only modify the time if the current time source has been set to *Manual*.
Time source	It is either *Manua*l, *NTP* or *GPS / NMEA.* The meaning of each configuration option is as follows: • *Manual*: The user configures the *Date* and *Time* fields manually. System date and time is controlled by the internal clock. • *NTP*: An external *Network Time Protocol* (NTP) server controls the value of the *Date* and *Time* fields. The system is synchronized with the server each time the equipment is restarted or when a new capture is run. • *Time reference*: The unit is configured to get the system time and date from the GNSS satellite systems tor ToD. This setting is available only if the unit has been properly configured to receive a a time reference based on any of these interfaces (See section 2.6).
UTC offset (hours)	This is the time difference in hours between your local time zone and the *Universal Time Coordinated* (UTC) time zone This setting makes sense only if *Time Source* has been configured to *NTP* or *Time reference*.

Table 12.9: Time Source Configuration Options

Setting	Description
UTC offset (min)	This is the value to be configured when the time offset between your local time zone and the UTC zone is not an integer value of hours. This setting makes sense only if *Time Source* has been configured to *NTP* or *Time reference*.
Locked	This is a read-only field that is set to *Yes* when the system clock is synchronized with the time announced in a NMEA interface.The value of *Locked* is *No* otherwise. Sometests requiring GPS / Glonass synchronization may require the system clock to be locked to the satellite system. This sense makes sense only if *Time Source* has been configured to *Time reference*.
NTP server	IP address or domain name corresponding to the NTP server you want to use to synchronize your unit. If you want to use a domain name for the server you need to make sure you have configured a DNS server in your network settings (See section 12.5.1). This setting makes sense only if *Time Source* has been configured to *NTP*.
NTP status	Displays the current status of the NTP server configured in the *NTP server* field. It is one of the following: • *Server not available*: The server configured in NTP server is not available. Make sure that your network interface is properly configured and that the server is accessible. • *Waiting*: The test unit is still waiting for a reply from the remote server. • *Synchronized*: The equipment is correctlysynchronized with the external server configured in *NTP server*. This is a not editable field. It is only active if *Time Source* has been configured to *NTP*.

To configure the system time and date in your test unit follow these steps:

1. From the *Home* panel, go to *System (*)*,
   The general system menu is displayed in the screen.
2. Select *General settings* to display the platform-wide configuration.
3. Go to *Clock setup*

4. Configure *Manual*, *NTP* or *Time reference* time and date with the help of the *Time source* field.
   Note: The *Time reference* setting requires that an appropriate clock input is enabled as a reference interface before configuring the system clock *Time source* (See section 2.6.2).
5. If you have configured *Time source* to *Manual* in the previous step, configure the *Date* and *Time* field to your local time and date. If *Time source* has been configured to *Time reference*, enter the *UTC offset (hours)*, *UTC offset (min).* If the configuration is to *NTP* then enter also the *NTP server* and wait for the equipment to establish synchronization with the server.

12.6.Using the Remote Control

The remote control application constitutes a remote graphical user interface that reproduces pixel by pixel the tester screen in virtually any remote device supporting the VNC protocol. This includes not only computers but also smartphones or tablets. The only requirements for the controlling devices are:

- IP connectivity with the tester. Any IP connection including Ethernet and WiFi should work.
- They must have a VNC client installed. Currently, there are VNC clients for most OS in the market. Some of them are free.

The remote control is an optional feature for Tempo that is supplied by Calnex with an special license.

Before using the remote control you need to configure the platform Ethernet interface and connect the equipment to the management network (See section 12.5.1). Once this is done, follow this procedure to use the remote control:

1. From the *Home* panel, go to *System*,
   The system configuration panel is displayed.
2. Select *General settings* to display miscellaneous system-wide settings, including the ones referred to the remote control.
3. Enable the remote control with the help of *Remote control*.
4. Optionally, supply a password with *Remote control password*. The password you configure here will be requested in all incoming VNC connections.
5. In the controlling device, run the VNC client and enter the password you have configured in *Remote control password* if you are requested to do so.

6. Use the keyboard or the mouse to browse the instrument panels, start measurements, insert events or any other action.

Table 12.10: Remote Control Keys

Key	Description
Home	It is equivalent to the HOME key. It displays the *Home* panel.
Esc	It is equivalent to the Esc key. It leaves the current panel and displays the previous one in the panel hierarchy.
Enter	It is equivalent to the ENTER key. It confirms settings.
Ctrl+L	It is equivalent to LEDS. It displays the *Leds* panel.
Ctrl+S	It is equivalent to SUM. it displays the *Summary* screen
Ctrl+R	It is equivalent to RUN. It starts / stops a measurement
Ctrl+E	It is equivalent to EVENT. It starts / stops event insertion

Appendix A
Technical Specification

A.1. General

1. Operation over two SFP/ SFP+ compatible interfaces and two 1 Gigabit Ethernet RJ45 connectors. Each set SFP / SFP+ and RJ-45 constitutes one logical port (Port A - Port B).
2. Supports concurrent synthetic traffic generation and analysis over Port A and Port B, including Ethernet / IP multistream traffic generation, PHY / ETH / IP / UDP traffic reflection and advanced QoS analysis.
3. Includes traffic generation and analysis features up to 10 Gb/s, equivalent to 15 millions of frames if frame size is set to 64 bytes. If the equipment is connected in through mode, it accepts and forwards frames at wire-speed.
4. Ability to disconnect traffic generation in each individual port (monitor mode) or to disable all processing in all protocol layers in each individual port (disabled mode).
5. Hardware acceleration for time critical protocols such as IEEE 1588 / PTP.
6. Multi-stream generation and support of multiple simultaneous filtering with specific filter statistics is supported.
7. The GNSS input has its own dedicated SMA port (GNSS).
8. Wire speed (1 Gb/s) traffic capture and protocol analysis in endpoint and pass-through modes of miscellaneous protocols including PTP, NTP.
9. Detailed latency analysis of IEC 61850 protocols such as GOOSE and SV.

A.2. Operation Modes

1. *L1 Endpoint operation:* Generation and analysis of PCS codes or any other pattern, framed or unframed required for BER testing at Layer 1.
2. *Ethernet Endpoint operation:* The equipment generates and receives Ethernet PCS codes and Ethernet frames (if required to do so) in port A and B.
3. *IP Endpoint operation:* The equipment generates and receives IPv4 and IPV6 datagrams in port A and B.

4. *Through operation:* The equipment does not generate traffic. Traffic received from port A is forwarded to port B. Traffic from port B is forwarded to port A.

A.3. Clock

1. Internal time reference better than ±2.0 ppm.
2. Optional OCXO internal reference better than ±0.1 ppm. Optional Rubidium internal reference.
3. Holdover operation in units equipped with OCXO and Rubidium references.

A.3.1. Rubidium Reference

1. Free running output freq. accuracy on shipment (25 ºC): ±5e-11
2. Aging (1 day, 24 hours warm up): ±4e-11
3. Aging (1 year): ±1.5e-9
4. Time accuracy to UTC (24 h locked to GNSS, peak value, ±2 ºC): ±40 ns.
5. Time accuracy to reference (24 h locked to 1PPS / ToD, peak value ±2 ºC): ±10 ns.
6. Holdover output time accuracy (2 hours, ±2 ºC): ±100 ns
7. Holdover output time accuracy (24 hours, ±2 ºC): ±1.0 µs / 1 day
8. Warm-up time (time to <1.5e-9): 15 minutes (typical, 25 ºC)

A.3.2. Built in GNSS

1. Compatibility with GPS, GLONASS, BeiDou and Galileo with single or multiple constellation selection.
2. Fixed position mode for GNSS references.
3. Automatic setting of UTC-to-TAI offset (leap second count) through GNSS.
4. 4V - 5V DC output in GNSS port to feed an external antenna.
5. Cable delay compensation.
6. Automatic antenna detection

A.3.3. GNSS Compact Antenna

1. SMA male connector
2. Polarization: RHCP
3. Frequency band: 1573 MHz - 1610 MHz
4. Gain: 27 dB
5. Noise figure: 1.5 dB
6. Voltage: 2.7 V - 5.5 V
7. Protection level: IP 67

A.3.4. Clock Reference Inputs

1. 10 MHz, 5 MHz, 2048 kb/s, 2048 kHz, 1544 kb/s, 1544 kHz (REF IN/OUT port).
2. 1 PPS, 1PP2S balanced (REF IN/OUT) and unbalanced (REF IN port) compatible with standard ITU-T G.8271. ToD balanced (REF IN/OUT) compatible with ITU-T G.8271, China Mobile and NMEA formats.
3. IRIG-B00X, B12X, B13X, B14X, B15X, B22X unbalanced (REF IN port). 50 Ω or high impedance modes. Up to 25 Vpp. AC or DC coupling. IRIG-B00X, B22X balanced (REF IN/OUT port). ITU-T V.11 electrical characteristics.
4. Ethernet through Port A and Port B (over any valid electrical / optical synchronous Ethernet interface).
5. Custom delay compensation for phase and time inputs.

A.3.5. Clock Reference Outputs

1. *2048 kHz* and *10 MHz* unbalanced (port C).
2. 1 PPS, 1 PP2S, balanced (REF IN/OUT) and unbalanced (REF OUT port) compatible with standard ITU-T G.8271. ToD balanced (REF IN/OUT) compatible with ITU-T G.8271 and NMEA.
3. IRIG-B00X, B12X, B13X, B14X, B15X, B22X unbalanced (REF OUT port). 50 Ω or high impedance modes. 5 Vpp. AC or DC coupling. IRIG-B00X, B22X balanced (REF IN/OUT port). ITU-T V.11 electrical characteristics.
4. Custom delay compensation for phase and time outputs.

A.4. Ethernet PHY

1. The following Ethernet interfaces are supported by the SFP / SFP+ ports: 10GBASE-SR, 10GBASE-LR, 10GBASE-ER, 10GBASE-T, 1000BASE-T, 1000BASE-SX, 1000BASE-LX, 1000BASE-ZX, 1000BASE-BX, 100BASE-FX, 100BASE-TX, 10GBASE-T.
2. The following Ethernet interfaces are supported by the RJ-45 ports: 10BASE-T, 100BASE-TX, 1000BASE-T.
3. Ability to enable or disable the light transmitter in optical interfaces.
4. Electrical ports compliant with IEEE 802.3. Electrical isolation 1500 V (rms).
5. SFP+ bay according with IEEE 802.3, Not isolated, +3.3 V (maximum).

A.4.1. Auto-Negotiation

1. Negotiation of bit rate. Allow 10 Mb/s, allow 100 Mb/s, allow 1000 Mb/s,.
2. Selection of clock master or slave roles in 1000BASE-T interface.
3. Ability to disable auto-negotiation and force line settings in 10 Mb/s, 100 M/s electrical interfaces and 1000 Mb/s optical interfaces.

A.4.2. Synchronous Ethernet

1. Interfaces: 100BASE-TX and 1000BASE-T (unidirectional) through the attached RJ-45 ports. Through external SFP / SFP+:10GBASE-SR, 10GBASE-LR, 10GBASE-ER, 1000BASE-T, 1000BASE-SX, 1000BASE-LX, 1000BASE-ZX, 1000BASE-BX, 100BASE-TX.
2. Operation: Analysis of synchronous Ethernet signal in *Ethernet endpoint*, *IP Endpoint* and *IP Through modes*, generation of synchronous Ethernet signal in *Ethernet endpoint* and *IP Endpoint* modes. Transparent synchronous Ethernet pass-through in *IP Through* mode.
3. Fixed frequency offset generation on transmitted signals with maximum value of ±120 ppm as per ITU-T O.174 (11/2009) 8.2.1.
4. Sinusoidal wander generation on Ethernet interfaces following ITU-T O.174 Amendment 1 sections 8.4.2.1 and 84.2.2 and ITU-T O.174 (11/2009) section 8.4.
5. Generation, decoding and transparent forwarding (*IP Through mode*) of the ESMC and the SSM code. Transmission and reception of “hear-beat” and event SSM messages is subject to ITU-T G.8264 clauses 11.3.2.1 and 11.3.2.2.
6. QL to be transported by the SSM is encoded as specified in ITU-T G.781 clauses 5.5.2.1 (Option I), 5.5.2.2 (Option II) and 5.5.2.3 (Option III).
7. SSM messages are generated at port level. Source MAC address is set to the local profile MAC address.

A.4.3. Power over Ethernet

1. PoE (IEEE 802.3af-2003) and PoE+ (IEEE 802.3at-2009) detection.
2. PoE interfaces: 10BASE-T, 100BASE-T and 1000BASE-TX through attached RJ-45 ports A and B.
3. PoE pass-through when the equipment is configured in transparent (through) operation mode.
4. PoE voltage between pairs 1-2 / 3-6 and 4-5 / 7-8 in endpoint test. Voltage and current in pairs 1-2/ 3-6 and 4-5 / 7-8 in through mode.

A.5. Ethernet MAC

1. Ethernet MAC generation and analysis in Ethernet and IP Endpoint mode. Analysis in Ethernet / IP Through mode.
2. Supported Ethernet frame formats: DIX, IEEE 802.1Q, IEEE 802.1ad.
3. Support for Jumbo frames with MTU up to 10 kB.
4. Setting of source and destination MAC addresses. For source MAC address, users can choose between the factory default address or a user custom address. Destination addresses can be configured as the opposite port factory default address, a single custom address or an address range. If they are specified as a range, the generated sequence will contain all the addresses within the configured range.

5. Setting of the Type / Length value in ordinary Ethernet frames. Configuration of the Type value is blocked if the user sets a frame structure requiring an specific Ethernet payload type.
6. Enable / disable VLAN and Q-in-Q modes. In VLAN mode, the Type / Length value is automatically set to 0x8100. In Q-in-Q mode, the Type / Length value is set to one of 0x88a8, 0x8100, 0x9100, 0x9200 or 0x9300.
7. Configuration of the VLAN VID and User Priority if the VLAN encapsulation is enabled.
8. In Q-in-Q mode, configuration of the S-VLAN VID, DEI and PCP. Configuration of the C-VLAN VID and User Priority.
9. Configuration of the frame size.
10. Insertion of FCS errors using the following insertion modes: single, burst, rate and random.

A.6. MPLS

1. MPLS generation and analysis in IP Endpoint mode. Analysis in Ethernet / IP Through mode.
2. Support of a single and double label stack (Top and Bottom with bottom of stack bit is set to 1 in Bottom label). The label is formatted as specified in RFC 3032.
3. Configuration of the TTL, exp and label fields for Top and Bottom MPLS headers.
4. If the MPLS block is enabled, the Type field of the MAC frame will be fixed to 0x8847 (unicast packets) or 0x8848 (multicast packets).

A.7. IPv4

1. IPv4 generation and analysis in IP Endpoint mode. Analysis in Ethernet / IP Through mode.
2. The Ethernet Type field is forced to 0x0800 value if IPv4 generation is enabled.
3. Configuration of source and destination addresses. Destination addresses can be configured as the opposite port factory current address, a single custom address or an address range. If they are specified as a range, the generated sequence will contain all the addresses within the configured range.
4. Configuration of destination MAC address either by hand or using ARP requests. The equipment generates ARP replies from a single, main IP address, configured in a port-specific local profile menu. All other ARP request messages are ignored.
5. Configuration of DSCP CoS labels, TTL and transport protocol. If transport protocol is UDP, support of UDP frame with source and destination port configuration.
6. Insertion of IP checksum errors (IP endpoint mode) using the following insertion modes: single, burst, rate and random. This event does not produce errors in lower transmission layers. Insertion of IP checksum errors requires regeneration of the FCS field.

A.8. Generic / /UDP Traffic Generator

1. Generation over 8 independent streams. Each stream has its own specific bandwidth profile and payload /pattern configuration.
2. Two independent traffic generators, one for each test port (Port A and Port B).

A.8.1. Bandwidth Profiles

1. Traffic can be generated in four different modes: *Continuous*, *Periodic burst*, *Ramp* and *Random*.
2. *Continuous* traffic is specified by a single parameter entered either as a percentage of the channel capacity, a value in b/s or a value in frames/s.
3. *Periodic* burst is specified by the following values: *High traffic* (%, b/s, frames/s), *Low traffic* (%, b/s, frames/s), *High duration* (frames, seconds) and *Low duration* (frames, seconds).
4. *Ramp* traffic is specified the following values: *High traffic* (%, b/s, frames/s), *Low traffic* (%, b/s, frames/s), *Steps* (integer number) and *Step duration*(seconds).
5. *Random* traffic is specified by the *Poisson* average traffic as a percentage, a value in b/s or a value in frames/s.

A.8.2. Test Patterns and Payloads

1. Layer 1 test patterns are available in *L1 endpoint* mode. All remaining patterns are available in IP endpoint and Ethernet endpoint modes.
2. Layer 1 BER test patterns from IEEE 802.3-2008 Annex 36A: HF test pattern, LF test pattern, MF test pattern, Long continuous random test pattern, Short continuous random test pattern.
3. Layer 1 BER test patterns IEEE 802.3-2012: PRBS 2^{31}-1, A-seed (LAN interfaces only), B-seed (LAN interfaces only),
4. Layer 2-4 BER test patterns: PRBS 2^{11}-1, PRBS 2^{15}-1, PRBS 2^{20}-1, PRBS 2^{23}-1, PRBS 2^{31}-1. These patters apply to stream 1 only.
5. Test payload for SLA statistics based in the ITU-T Y.1731 vendor specific OAM payload (Layer 2 tests) or a proprietary ATSL format (Layer 3 tests). The SLA payload for Layer 2 tests configures the Ethertype field to the default value of 0x8902 (IEEE 802.1ag / ITU-T Y.1731 OAM).
6. All zeros test pattern.
7. Insertion of TSE (endpoint modes) using the following insertion modes: *single*, *rate* and *random* (only in bit patterns or payloads containing bit patterns). Insertion of TSE requires regeneration of FCS (and UDP CRC if configured).

A.9. Filter

1. Up to 8 simultaneous filters per port can be applied to the traffic.

2. The decision of which branch is in charge of processing traffic is taken for each individual frame using one or several filters. Each frame is processed by one and only one branch. If there is a conflict, the branch with smaller index has precedence.
3. Selection is done by using the Ethernet frame fields. If the Ethernet frame carries IP it is possible to select frames by the IP header fields. In such cases when the Ethernet frames carry IP traffic it is possible to select frames by the contents of higher lever protocols of the TCP/IP stack.
4. The equipment supports a generic filter which can select frames by using a 16 bit mask and an arbitrary offset defined by the user.

A.9.1. Ethernet Selection

1. By source and destination MAC addresses. Selection of MAC address sets with masks.
2. By Type / Length value with selection mask.
3. By C-VID and S-VID with selection mask.
4. By Service and Customer priority code-point value with selection mask.

A.9.2. MPLS Selection

1. Separated filters to account for the Top and Bottom MPLS headers.
2. By label value. Specific option for selection of label ranges.
3. By the value of the Exp field with specific option for selection of ranges.

A.9.3. IPv4 Selection

1. Selection by IPv4 source or destination address. Or both at the same time. It is possible to select address sets by using masks.
2. Selection by protocol as defined in the IPv4 datagram protocol field.
3. Selection by the DSCP fields, it is possible to filter single DSCP values or DSCP value ranges.

A.9.4. IPv6 Selection

1. Selection by IPv6 source or destination address (or both at the same time). It is possible to select address sets by using masks.
2. Selection by IPv6 flow label. Selection based on the next header field value. Selection by DSCP.

A.9.5. UDP / TCP Selection

1. Selection by UDP or TCP port. Either single value filters or filtering of port ranges is available.

A.9.6. Protocol Selection

1. Selection by protocol applying to the following protocols: IEEE 1588-2008 over Ethernet, IEEE 1588-2008 over IPv4, NTP, IEEE 61850 GOOSE and SV.
2. Selection by Domain, Port Identity and Message Type (*Sync*, *Delay Request*, *Delay Response*, *Peer Delay Request*, *Peer Delay Response*, *Follow up*, *Peer Delay Follow up*, *Announce*, *Signaling*, *Management*) when the selected protocol is IEEE-1588.
3. Packet filtering based on NTP message type (*Symmetric active*, *Symmetric passive*, *Client*, *Server*, *Broadcast*, *Control*, *Other*) when the selected protocol is NTP.
4. Selection by APPID when the protocol is IEC 61850.

A.10. PTP / IEEE 1588

1. PTP emulation and monitoring in Ethernet and IP Endpoint modes (Port A). PTP monitoring in Ethernet / IP Through mode (Ports A and B).
2. Support of hardware-assisted generation and decoding of Precision Time Protocol (PTP) as defined in IEEE 1588-2008.
3. Operation and equipment connection to the network is as any IEEE 1588 Ordinary Clock.
4. Both *Master* and *Slave* operations are supported in endpoint mode. Ability to force Slave or Master roles.
5. Encapsulations: PTP over UDP over IPv4 (IP Endpoint mode) as defined in IEEE 1588-2008 Annex D, PTP over IEEE 802.3 / Ethernet as defined in IEEE 1588-2008 Annex F.
6. Compatible with unicast, multicast and hybrid transmission with UDP and Ethernet payloads. Supports unicast negotiation.
7. Support of 1-step and 2-step clock modes both in slave or master emulation.
8. Support of peer-to-peer and end-to-end delay mechanisms.
9. Configuration of Domain, Priority 1, Priority 2 and Clock class. Configuration of announced capabilities: UTC offset, time and frequency traceability, time-scale and time source.
10. Setting of message rates for Sync, Delay Request, Peer Delay Request and Announce messages. Configuration of Announce message time-out.

A.11. NTP

1. NTPv3 / NTPv4 server and client emulation. Test mode to verify performance of NTPv3 / NTPv4 servers.
2. Support of hardware-assisted time stamping for Network Time Protocol (NTP).
3. Configuration of protocol version, server address (IP address or domain name) and polling interval in client emulation and test modes

4. Configuration of protocol version, stratum level and reference id in master emulation mode.

A.12. PHY Results

A.12.1. Cable Tests

1. For inactive links: Open/short fault indication and distance to fault in meters (accuracy: 1 m).
2. For 10/100 Mb/s active links, the following results are reported: current local port MDI/MDI-X status.
3. For 1 Gb/s active links the following results are reported: current local port MDI/MDI-X status, pair polarities (normal/inverted), pair skew (ns).

A.12.2. SFP

1. SFP presence, current interface, vendor, and part number.
2. Optical power measurement (transmitted and received power) over compatible SFP transceivers.

A.12.3. Auto-Negotiation

1. Auto-negotiation results with current bit rate and duplex mode.
2. For 1000BASE-T indication of clock *Master* and *Slave* roles

A.12.4. Synchronous Ethernet

1. Measurement of the line frequency (MHz), frequency offset (ppm) and frequency drift (ppm/s) as specified in ITU-T O.174 (11/2009) clause 10.
2. TIE / MTIE / TDEV measurement on Ethernet interfaces following ITU-T O.172 clause 10 and sampling frequency of 50 Hz.
3. Decoding of the QL transported in SSM as per ITU-T G.781 clauses 5.5.3.1 (Option I), 5.5.3.2 (Option II) and 5.5.3.3 (Option III).

A.13.Frame Analysis

1. Simultaneous per port statistics.

A.13.1. Ethernet Statistics

1. Frame counts: Ethernet, IEEE 802.1Q (VLAN), IEEE 802.1ad frames, Q-in-Q frames, control frames, pause frames.
2. Frame counts: unicast, multicast and broadcast.
3. Basic error analysis: FCS errors, undersized frames, oversized frames, fragments, jabbers.

4. Frame size counts: 64 or less, 65-127, 128-255, 256-511, 512-1023, 1024-1518, 1519-1522, 1523-1526 and 1527-MTU bytes.

A.13.2. MPLS Statistics

- MPLS stack length: minimum, maximum.

A.13.3. IP Statistics

1. Packet counts: IPv4 packets, IPv6 packets.
2. Packet counts: unicast, multicast and broadcast.
3. TCP packets, UDP packets, ICMP packets.
4. IPv4 checksum errors, IPv6 checksum errors.
5. UDP and TCP checksum errors.

A.13.4. Bandwidth Statistics

1. Simultaneous per port and per stream statistics
2. Current, maximum, minimum Ethernet traffic expressed in bits per second, frames per second and a percentage of the nominal channel capacity.
3. Ethernet unicast, multicast and broadcast traffic expressed as a percentage of the nominal channel capacity.
4. IPv4 and IPv6 statistics expressed in bits per second, frames per second and a percentage of the nominal channel capacity.
5. UDP traffic expressed in bits per second, frames per second and a percentage of the nominal channel capacity.

A.13.5. SLA Statistics

1. Simultaneous per stream and per port statistics.
2. Delay statistics are provided by means the point-to-point, Ethernet frame transfer delay (FTD): current, minimum, maximum, and mean values. FTD statistics follow definitions given in ITU-T Y.1563
3. Delay variation statistics are provided by the following statistics: standard deviation of the FTD, peak FDV (difference between maximum FDV and minimum FDV), current jitter (smoothed value of the jitter following RFC 1889 and RFC 3393), maximum jitter, mean jitter.
4. Frame reordering and duplication statistics (RFC 5236): Out-of-order frames, Out-of-order frame ratio, duplicated frames, duplicated frame ratio.
5. Frame loss statistics to be used is the lost frames count and the 2-way Ethernet Frame Loss Ratio (FLR).
6. Availability statistics: Severely Errored Seconds (SES) count, Percent Ethernet service Unavailability (PEU), Percent Ethernet service Availability (PEA).

A.13.6. Service Disruption Time

1. Simultaneous per port statistics. Analysis carried out over flow 1 statically.

2. Service Disruption test based on the analysis of the SLA pattern carried by a synthetic traffic flow.
3. Resolution is 1 ms.
4. Statistics are service disruption events count. Total disrupted time. Average, minimum and maximum time in a service disruption event. Time in the last disruption event.

A.13.7. BER

1. Simultaneous per port statistics. Analysis carried out over flow 1 statically.
2. Bit error count, seconds with errors, bit error ratio (BER).
3. Pattern losses, pattern loss seconds.

A.13.8. Network Exploration

1. Simultaneous per port results for a single search field.
2. Top talkers statistics: Displays the 16 most common source MAC addresses (Ethernet Endpoint mode) or source MAC / IPv4 / IPv6 addresses (IP Endpoint mode).
3. Top VID (IEEE 802.1Q) statistics: Displays the 16 most common VID tags.
4. Top S-VID (IEEE 802.1ad) statistics: Displays the 16 most common S-VID tags.
5. Automatic setup of the eight available filtering blocks to match the items found in the top talkers list.

A.14. PTP / IEEE 1588 Statistics

1. Protocol state details: *port state*, *best master clock protocol state*, *master identity*, *grandmaster identity*, *grandmaster BMC priorities*, *grandmaster clock class*, *grandmaster accuracy*, *grandmaster clock variance*, *grandmaster time source*, *master IP* or *Ethernet address.*
2. TX and RX PTP frame counts classified by frame type: *Sync*, *Delay request*, *Delay response*, *Peer delay request*, *Peer delay response*, *Follow up*, *Peer delay response follow up*, *Announce*, *Signaling*, *Management*.
3. *Sync message packet delay* statistics: *Current*, *maximum*, *minimum*, *average*, *standard deviation* and *range* of the delay. *Current*, *maximum* and *average Sync* packed delay variation.
4. *Sync Inter Arrival time* analysis: Average and current.
5. Delay request message delay statistics: *current*, *minimum*, *maximum*, *average*, *standard deviation* and *range*.
6. *Round trip delay* computed with the path delay mechanism: *Current* and *mean* values.
7. *Correction field statistics*: current, maximum and average.

8. Sync floor delay packet population metrics (ITU-T G.8260): *Sync Floor Packet Count* (FPC), *Floor Packet Rate* (FPR) and *Floor Packet Percent* (FPP). Configurable Pass / Fail threshold for FPP performance metric.
9. *Wander metrics*: TIE (ITU-T G.8260 *pktfilteredTIE*), MTIE (ITU-T G.8260 *pktfilteredMTIE*) and TDEV (ITU-T G.8260 *pktfilteredTDEV*) with user configurable rating masks..
10. Two-way TE and max |TE| measurement with user defined pass / fail thresholds.
11. Low frequency TE and high frequency TE components with user defined pass / fail thresholds..
12. Path Delay Asymmetry Between PTP master and client clocks
13. Frequency offset measurement

A.15. NTP Statistics

1. Protocol status: *Port state*, *Stratum*, *Reference id*, *Polling interval*, *Root delay*, *Root dispersion*, *Leap status*, *Time.*
2. Message statistics. Count of transmitted and received *Symmetric active*, *Symmetric passive*, *Client*, *Server*, *Broadcast*, *Control* and *Other* packet types.
3. Delay statistics. Displays current value, mean, range and standard deviation of the following parameters: *Offset (theta)*, *Delay (delta)*, *Forward path delay*, *Return path delay*, *Asymmetry* Displays current value, mean and range of the *Jitter (psi)*.
4. Two-way Time Error statistics. Computes the following TE statistics: current value, mean, minimum, maximum, standard deviation.

A.16. Automatic Tests

1. The equipment supports automatic normalized tests defined in IETF RFC 2544 and ITU-T Y.1564.
2. Custom pass / fail objectives.
3. User configurable analysis port in symmetric tests.
4. Static Port A operation in asymmetric tests.

A.16.1. IETF RFC 2544 Test

1. Compatible with Ethernet Endpoint and IP Endpoint modes.
2. Support throughput, frame-loss, latency, back-to-back and recovery time tests.

A.16.2. ITU-T Y.1564 Test

1. Supports the Ethernet service activation methodology defined in ITU-T Y.1564 when the equipment is configured in Ethernet Endpoint and IP Endpoint modes.
2. Testing of up to eight services (non-color aware mode) or up to four services (color aware mode) with configuration of the *CIR*, and *EIR* for each of them.

3. Configuration of *frame delay* (FTD), *frame delay variation* (FDV), *frame loss ratio* (FLR) and availability objectives for each service to be verified.
4. Settings for test phase 1 (Network Configuration Test) are S*teps* (integer number) and *Step duration* (seconds). Settings for phase 2 (Ethernet Service Test) are the *Phase duration* and *bandwidth profile* (*deterministic*, *random*).
5. The test bandwidth profile for test phase 1 is a modified ramp where the *CIR*, *EIR* and *maximum throughput* rates are forced and the other transmission rates are derived from the *Steps* setting. For phase 2, the test bandwidth profile is deterministic / random generated at the CIR bit rate for all services at the same time.
6. The FTD, FDV (mean value) and FLR is measured for each step in phase 1 and phase 2 and a pass / fail indication is computed for each step. Phase 1 fails if there is at least one failed result in this phase. Phase 2 does not start is phase 1 fails.

A.16.3. IETF RFC 6349 Test

1. Operation modes: active (client) or passive (server).
2. Accepted endpoints in client mode: Calnex and IPerf3.
3. Allows user configuration of the MTU and MSS.
4. User configuration of the Bottleneck Bandwidth (BB) in frames/s or as a percentage of the nominal link capacity.
5. Measurement of the Round-Trip Time (RTT) based on the mechanism described in RFC 2544 through a single UDP stream.
6. Window sweep test at four different window sizes: 25%, 50%, 75% and 100% of the BDP.
7. Measurement of the Transfer Time ratio, TCP Efficiency and Buffer delay as defined in RFC 6349 4.1, 4.2 and 4.3.

A.17. Port Loopback

1. Layer 1-4 loopback.
2. Loop frames matching current filtering conditions or loop all frames in layer 2-4 loopbacks.
3. Loop controls for broadcast and ICMP frames.

A.18. ICMP Processor

1. Generation of on demand ICMP echo request (RFC 792) messages with custom destination IP address, packet length and packet generation interval.
2. Analysis of ICMP echo reply (RFC 792) messages with measurement of round trip time and lost packets.

3. Analysis of I*CMP Time-To-Live Exceeded* and *ICMP Port unreachable* replies received in the traceroute test.

A.19. Protocol Processor

1. IPv4 ARP (IETF RFC 826) for automatic resolution of remote MAC address in IP Endpoint mode (IPv4 network protocol).
2. IPv4 destination address resolution through DNS (IP Endpoint mode).
3. DHCP (client side) (IETF RFC 2131) for IPv4 profile auto-configuration or static IPv4 profile configuration.
4. Support of the Trace-route application over IPv4 using UDP packet transmission with increasingly higher TTL values. Support of the Trace-route application over IPv4 using ICMP echo request packets with increasingly higher TTL values.

A.20. Protocol Analysis

1. Simultaneous per filter and per port capture. Each packet is marked by the capture filter so that this filter could be identified at a later stage.
2. Capture of transmitted and received streams (port A and B) in endpoint configurations.
3. Capture of received streams (port A and B) in pass-through configurations at all speeds.
4. Simultaneous capture of transmitted and received frames.
5. Storage capacity: 256 MB.
6. Wrap around mode for continuous captures.
7. Export results to PCAP and PCAPNG formats.
8. Hardware time stamping of captured packets. Resolution is 1 ns.
9. Supports UTC time stamps when is connected to an external time clock reference input (GNSS, ToD or IRIG-B) or in holdover.
10. Decoding of the following protocols mapped over Ethernet: *SLA payload* (Calnex proprietary), *ESMC*, *ARP* and *Pause*.
11. Decoding of the following protocols mapped over IP: *SLA payload* (Calnex proprietary), *NTP, IGMP*, *DHCP*, *DNS* and *ICMP*.
12. Decoding of PTP over Ethernet and PTP over IP /UDP. Decoding of IEC 61850 GOOSE and SV protocols over Ethernet.
13. Packet-by-packet latency measurements for the following protocols: SLA payload (Calnex proprietary), IEEE 1588-2008, NTP, IEC 61850 GOOSE, IEC 61850 SV.

A.21. Platform

1. Size: 260 x 160 x 63 mm.
2. Weight: 1.9 kg (two battery packs).
3. Screen: 8 inch, TFT color (800 x 480 pixels).
4. USB type A port, according USB standard 2.0, DC output: +5 V / 0.5 A (max).
5. RS-232 / V.24 console port for maintenance tasks.

A.21.1. Power Specifications

1. Operation time with batteries (LiPO): 5 ~ 8 hours.
2. Battery recharge time (LiPO): 4 hours.
3. DC input, 12 V (nominal), 15 V (maximum) / 5 A (maximum).
4. External AC power adapter 100 - 240 V ~50 / 60 Hz, 1.5 A. Output 12 V DC, 5 A.
5. AC power grid fluctuations < ±10% of the nominal voltage.
6. Over-voltage category II.

A.21.2. User Interface

1. Graphical user interface controlled by touch-screen, keyboard or mouse.
2. Web based report and configuration file management.
3. Full remote control: SNMP or VNC.

A.21.3. Results

1. Storage in TXT and PDF file formats.
2. File transfer to SD card and USB port.
3. File management through web interface and SNMP.
4. Configuration and report storage and export through attached USB port.

A.21.4. Operational Ranges

1. Operational range: -10ºC to +45ºC.
2. Storage range: -20ºC to +70ºC.
3. Operation humidity: 5% - 95%.
4. Height: Up to 3000 m above the sea level.
5. Pollution degree II.

Appendix B
Common Issues and Solutions

The following table summarizes some common configuration issues related with everyday use of Tempo. Some of them are applicable only to a very specific situations but some others are valid as a general use advises. For example it is always better to use the local IP address as the source address for test traffic than an spoofed (manual) address whenever is possible.

Table B.1:

Issue	Solution
DHCP does not work	• Make sure that the network supports DHCP configuration and that your equipment is authorized to get a DHCP lease from the server. • In some situations Tempo DHCP address config- uration may be slow. The user can force imme- diate address negotiation by disabling DHCP for one moment and enabling it again.
Ping / Traceroute tests not available	• These are IP tests they are available only if the unit operation mode is set to IP endpoint mode.
eSAM, RFC 2544 or SLA test results are not available.	• eSAM, RFC 2544 or SLA analysis is active either in Port A results or in Port B results but never in both ports at the same time. Make sure that your test method settings (one-way or two way) are correct.
BER test results are not available	• BER testing require an special test payload. Configure the BERT payload in the *Payload* sub-menu within the port specific setup menu. Depending on your test setup you may need to configure the Port A and Port B payload to BERT.

Table B.1:

Issue	Solution
The unit is unable to establish link	• The test interface is configured in optical mode but you are using an electrical connector or the equipment is configured in electrical mode but you are using an electrical connector: Configure the right connector for your test by means the *Physical layer* settings in the port specific configuration menu. • You are using the optical interface but the light source is off. Please, remember that for security reasons the optical source is never enabled when the equipment is restarted. Make sure that the optical source is enabled in your optical tests. • The test interface does not support auto-negotiation but the equipment is configured to operate with auto-negotiation. The solution in this case is to disable auto-negotiation and force the bit rate to 10 or 100 Mb/s.
ARP does not resolve any destination MAC address. requests	• Your local proflie contains wrong settings. Your Tempo unit decides where to send ARP using your local IP address, subnet mask and default gateway configuration. If there is an error with these settings your requests will be lost in the network or the destination will be unable to send the reply back to the origin. Make sure that your local profile contains the correct configuration. • ARP requests are encapsulated in a wrong frame structure. For example, the network may be unable to process standard Ethernet frames if it is waiting for VLAN tagged frames. Make sure that you are using the correct encapsulation. • ARP requests are delivered to unsupported VLANs. Make sure that you configure the correct VIDs in your frames.

Table B.1:

Issue	Solution
Test traffic is not transmitted through a switch	• Configuration for testing through a switch is more simple than for a router but you still need to check that you have configured the right destination MAC address, encapsulation and correct VLAN tags in the *Frame layer* menu. If you have configured a two-way test and in the remote end you have a traffic reflector, you have to configure the remote device MAC address as the destination address for your streams. If you use Port B as the traffic analyser in a one-way test, you have to configure the Port B MAC address as the destination address for your traffic streams.
Test traffic is not transmitted through a router	• You are using an incorrect MAC destination address. When you transmit data through a router the destination MAC address has to be configured to the router MAC address corresponding to the interface you are connected with. The easiest is to configure ARP in *Frame layer* settings and leave the tester auto-configure the right destination MAC address. • You are using a wrong frame encapsulation in your *Frame layer* settings. Make sure that you are using the correct encapsulation (VLAN, Q-in-Q, IEEE 802.1ad). • You are using incorrect IP settings in *Local profile* and *Network settings*. Your local profile should contain a unique IPv4 address. The default gateway must be placed in your local network (the network prefix should match the network prefix of your IP address). The remote address should be routable from the tester. For example you can not send traffic to a private address behind a NAT filter from the Internet. • The remote host should be able to reply to ARP requests. Note that Tempo is unable to respond to ARP requests from addresses different to the local one. In case you need to receive test traffic in addresses different from the local one, you will need to configure static ARP entries in the router.

Table B.1:

Issue	Solution
No traffic detected in Filters panel.	• The traffic is being lost somewhere in the network. Use the global result statistics to know if this is the case. Make sure that the remote loopback device (if used) is properly configured. Check the *Network layer* (destination IP address), the *Frame layer* (destination MAC address, encapsulation, VLAN tags) and *Local profile* (IPv4 address, network mask, gateway and DNS server). The network will fail to send the test data to the destination if destination addresses and VID values are not configured to the right values. • You are receiving test traffic but filtering is not working properly. Use the *Match TX* setting in your filter configuration if you know that the network is not modifying the traffic in some way (CoS re-labelling, port modification in NAT filters or others). If the network is modifying the traffic, use a *Custom* filter instead.
All SLA test results are zero	• You may have a problem with the filter configuration. See how to solve problem with the filters (*No traffic detected in Filters*) • SLA results are computed only if you configure an special SLA payload in the generator and the analyser. for all your streams . You can set the SLA payload with the help of the *Payload* menu within the Port A setup. If you are using Port B as a traffic analyser, you will need to configure SLA payload in this port as well.
eSAM test fails to start	• If you are running a color-aware test the eSAM requires the green and yellow markers to have a different value for each service. For example, if you are using the VLAN priority bits as the color marker and you configure the green traffic priority bits to “1” in service number 1, then you have to configure the same field to something different to “1” for yellow traffic in the same service. Note that you can still configure the yellow traffic priority bits to “1” in services 2, 3 and 4.

Issue	Solution
eSAM Policing test always fails.	• You are running a policing test but there is not a traffic admission mechanism configured in the network. The eSAM policing test is designed to test this mechanism and it fails if not conforming traffic is not dropped. If you want to avoid the eSAM test to fail for this reason you have to disable the policing test using the *Policing test* control in the *eSAM* menu.
eSAM or RFC 2544 test returns a *No traffic* message.	• If you are testing through a switched network, you may be using incorrect *Frame layer* settings. Check the solution on how to proceed when *Test traffic is not transmitted through a switch.* • If you are testing through a routed network, you may be using incorrect *Local profile* or *Network layer* settings. Check the solution about how to proceed when *Test traffic is not transmitted through a router.* • The network may be re-labelling traffic or modifying the test traffic in some way. Check the solution about how to proceed when *No traffic detected in Filters panel.*