

Field Test Plan for Frequency Synchronization using NTP

Calnex Sentinel




More than 200,000 NTP base stations have been deployed globally for 3G networks. With increasing traffic levels, more and more intermittent issues such as dropped calls, handover failures and slow data transfers are showing up.

This document provides field test procedures to ensure high quality synchronization for 3G mobile backhaul networks running the NTP protocol for timing synchronization.

This test plan is applicable to Ericsson NTP base stations, supporting specific limits for Ericsson NTP clients and Ericsson NodeB devices, and other similar cell site routers/PTN equipments.

Contents

1	Background	3
2	Test Setup	4
3	Sentinel Configuration	5
3.1	Operating Mode	5
3.2	Measurement Mode	5
3.3	Time Base	6
3.4	Physical Interface Setup	7
3.5	NTP Server Selection	8
3.6	Packet Selection for FPP Measurements to G.8261.1	9
3.7	Vendor Specific Network PDV Distribution (PDD) Pass/Fail Criteria	10
3.8	Select Recovered Clock Mask	10
3.9	Signal Check	11
3.10	Start the Test	11
4	Measurement Results Display	12
5	Test Cases	13
5.1	Packet Delay Distribution (PDD) Analysis	13
5.2	Network PDV to ITU-T G.8261.1	15
5.3	Recovered Clock Stability to ITU-T G.8261.1	16
5.4	NTP Packet to Packet PDV Capture	18
6	Test Results Interpretation	19
6.1	With Client Clock Output	19
6.2	Without Client Clock Output	19
7	Offline Analysis and Report Generation using CAT	20
7.1	Import Results	20
7.2	Select Metrics	21
7.3	Generate a Report	22
	Appendix A: NTP Synchronization Technology	23
	Appendix B: Example Ericsson RBS PDD limits	26
	Appendix C: ITU-T Recommended Network Limits for Packet Networks	27
	Appendix D: ITU-T Recommended Client Clock Network Limits	28
	Appendix E: Example Generated Report	29

 **Note:** Measurement data shown in this document can be imported to the Calnex Analysis Tool (CAT) for more detailed analysis. CAT is available on all Calnex Paragon and Sentinel products.




1 Background

Frequency synchronization is critical for all mobile technologies.

The requirements for different mobile technologies are listed in the table below.

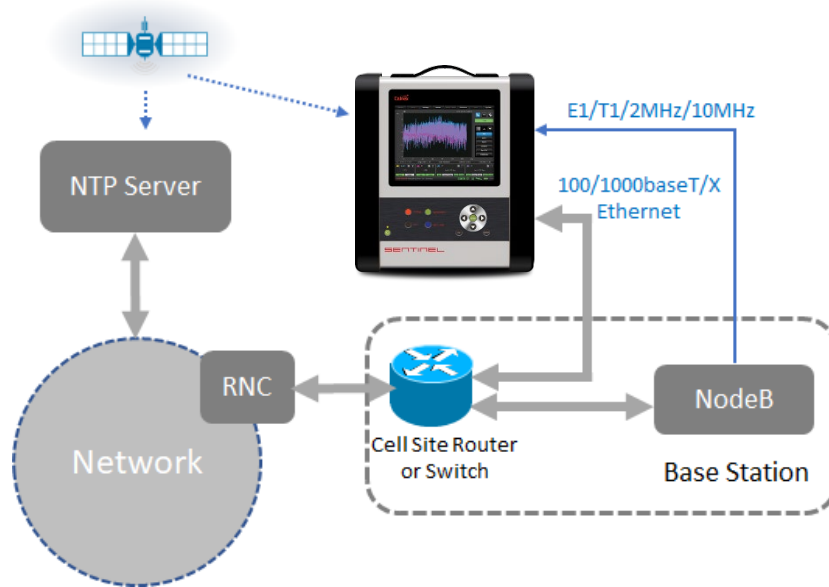
Application	Frequency	Time	Packet Backhaul Spec
CDMA2000	±50 ppb	±3 to 10 µs	
TD-SCDMA	±50 ppb	±1.5 µs	
GSM	±50 ppb	n/a	±16 ppb (G.8261.1)
WCDMA	±50 ppb	n/a	±16 ppb (G.8261.1)
LTE (FDD)	±50 ppb	n/a	±16 ppb (G.8261.1)
LTE (TDD)	±50 ppb	±1.5 µs (<3 km cell radius) ±5 µs (<3 km cell radius)	±16 ppb (G.8261) ±1.1 µs (for ±1.5 µs G.8271.1)
LTE-A MBSFN	±50 ppb	±1 to 5 µs Implementation dependent	±16 ppb (G.8261.1) ±1.1 µs (for ±1.5 µs G.8271.1)
LTE-A CoMP	±50 ppb		
LTE-A eICIC	±50 ppb		
Small Cells	±100 ppb	n/a (FDD) ±1.5 µs (TDD) ±1 to 5 µs (eICIC)	±33 ppb ±1.1 µs (for ±1.5µs G.8271.1)
Home Cells	±250 ppb	n/a (FDD) ±1.5 µS (TDD)	±100 ppb ±1.1 µs (for ±1.5 µs G.8271.1)

 **Note:** The 50 ppb stability requirement is at the Air interface. For the mobile backhaul, it is accepted that this translates to a requirement of 16 ppb. For small cells, the requirements are 100 ppb at the Air interface and 33 ppb for the mobile backhaul.

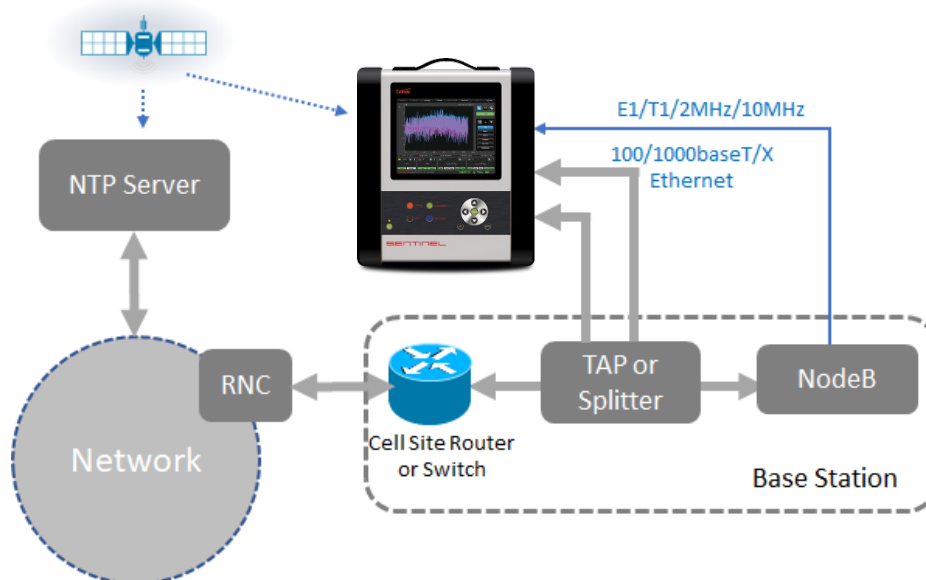
2 Test Setup

Sentinel can operate as a pseudo NTP Client connecting to the edge router and communicating with the remote NTP Server or in Monitor Mode connecting to an electrical TAP or an optical splitter to check the communication of the NodeB NTP Client and remote NTP Server. At the same time, the recovered clock from the NTP¹ Client can be output to Sentinel for wander measurements. The actual output clock interface will be vendor-specific. Common interfaces are E1/T1/2MHz/10MHz.

Typical field test setups using Sentinel are shown below:



Pseudo NTP Client Mode



¹ See Appendix A

3 Sentinel Configuration

Before performing any measurements, follow the steps below.

3.1 Operating Mode

From the **Mode** page configure Sentinel operating mode. For Pseudo NTP client operation select one channel as **SyncE / NTP Client**, for monitor mode select **NTP Monitor Mode**. If a recovered clock is being tested, select one of the **CLOCK** channels.



NOTE: Each clock module supports the simultaneous measurement of 2 input clocks with frequencies ranging from 0.5Hz to 200MHz.

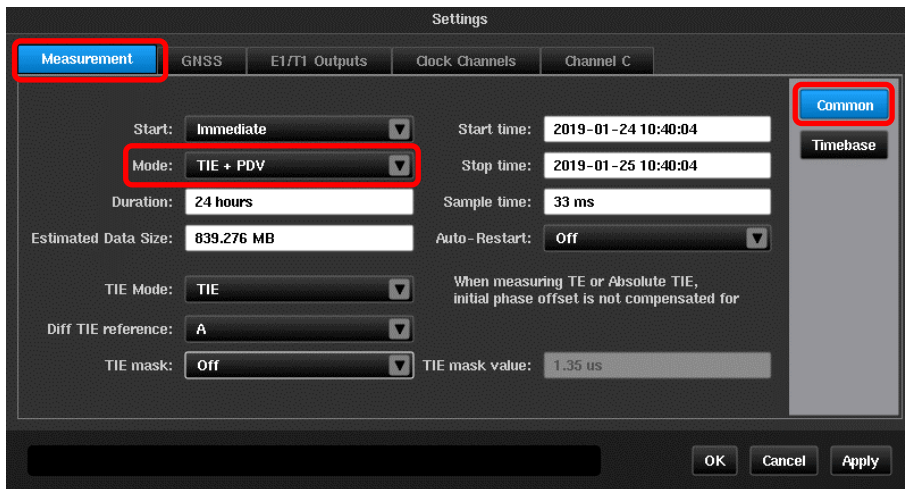
NOTE: Running in monitor mode requires 2 packet modules.

NOTE: If not operating in monitor mode packet modules can be configured for any combination of NTP Client or PTP Slave operation.

3.2 Measurement Mode

From the main GUI display window, select **Settings > Measurement > Common**.

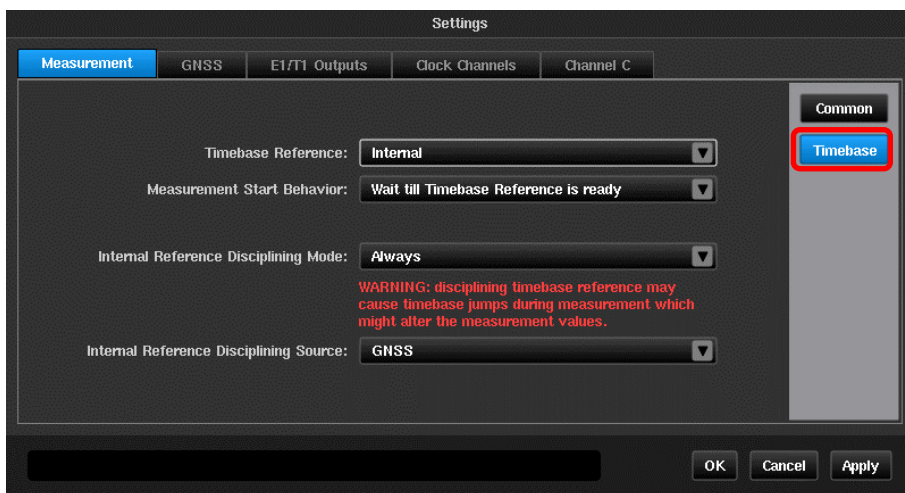
Set **Mode** to **TIE + PDV** and set the required test duration. The recommended test duration is 24 hours for normal network performance test. If intermittent issues occur in the network, a longer test duration may be required in order to capture the intermittent issues.



3.3 Time Base

Set Sentinel to use **Internal** clock as its **Timebase reference** and choose **GNSS** signal as the **Internal Reference Disciplining Source**. Set **Measurement Start Behavior** to **Wait till Timebase Reference is ready**, and **Internal Reference Disciplining Mode** to **Always** if a GNSS reference is available. Otherwise, set to **Not during the measurement** if no reference is available.


For other options of time configurations, please consult the Sentinel user manual²

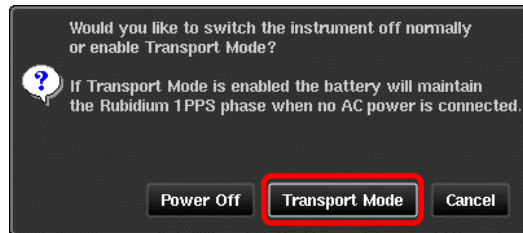


NOTE: From a cold start, it takes around 15 minutes for the internal Rubidium timebase to warm up. With the GNSS antenna connected, the GNSS receiver needs to lock to at least 3 satellites before it can output a valid reference to the Rubidium for disciplining. If less than 3 satellites are locked, the Rubidium will go into holdover.

NOTE: If no GNSS signal is available at the test site, the internal Rubidium can be disciplined in advance by applying a GNSS signal in the lab before going on site. The embedded battery on the Sentinel will keep the Rubidium in holdover during the transportation from lab to the field by setting Sentinel into transport mode. To achieve high accuracy, it is recommended to train the Rubidium in the lab for at least 12 hours. If Sentinel was last disciplined less than a week ago, this time can be shortened to 6 hours.

² Calnex Document CX3001

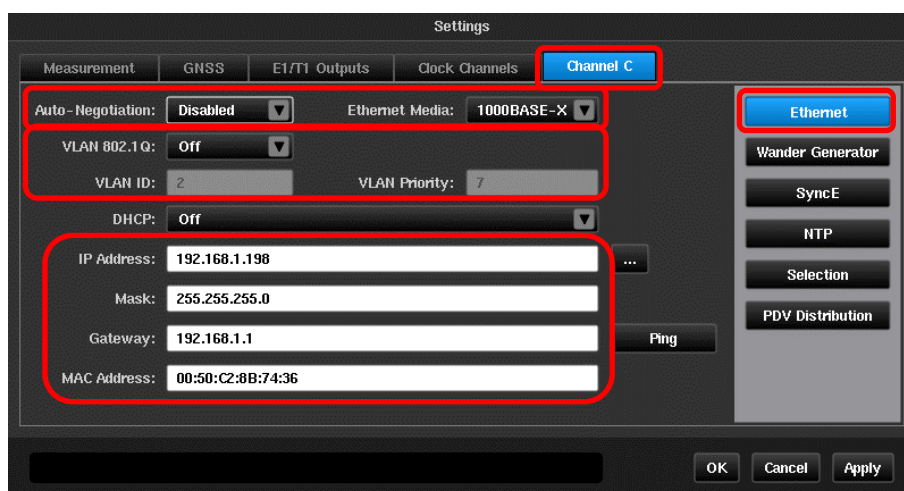
NOTE: To put Sentinel in Transport Mode, press the  button on the front panel. The following window will be displayed. Click on **Transport Mode**.



NOTE: Without mains power supply, the battery can keep the internal Rubidium powered for up to 3 hours. Once mains power is supplied again, the Rubidium will be powered by the main supply and the battery will start to re-charge.

3.4 Physical Interface Setup

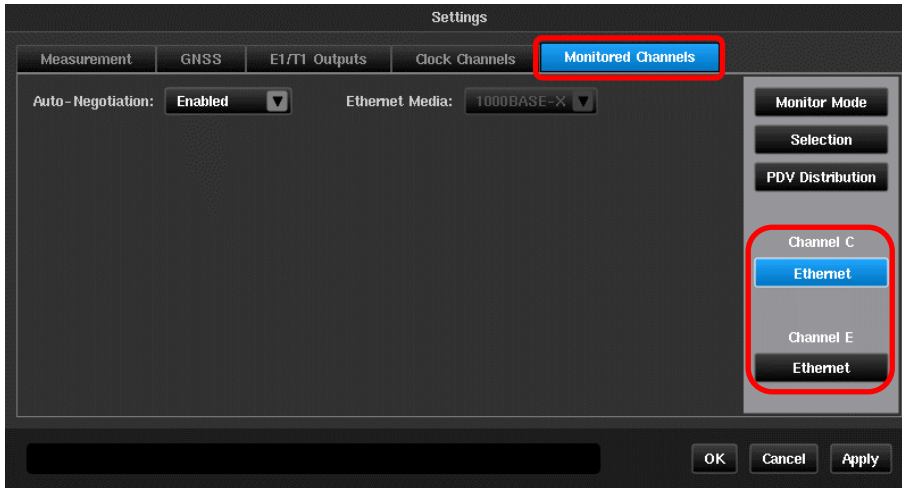
Each packet module that is being used should be configured to match the media that it is connected to. For NTP Pseudo Client mode this is done through the **Settings > Channel x > Ethernet** page.



Ensure that the physical media properties match the properties of the port being connected to. Any required VLAN configuration should be entered. If a DHCP server is not being used then the IP properties should be manually entered.

NOTE: Prior to testing, an IP address should have been provisioned by the operator along with details of the network mask and gateway address.

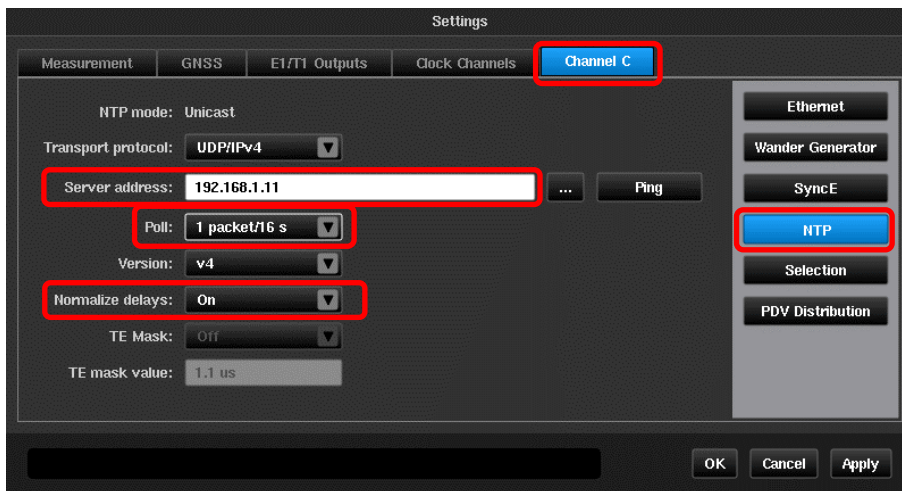
For monitor mode the media properties can be set through the **Settings > Monitored Channels > Ethernet** page.



There is an Ethernet page for both channels used and these should be set to the same values. Electrical TAPs may require **Auto-Negotiation** to be **Enabled** while optical splitters generally require a fixed rate to be entered.

3.5 NTP Server Selection

In Pseudo NTP Client mode the NTP Server properties are entered in the **Settings > Channel x > NTP** page.

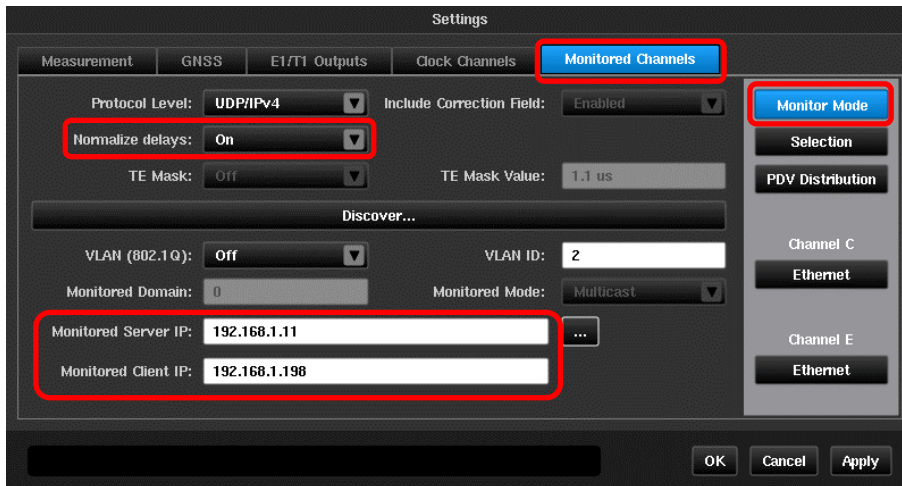


Set the **Server address** and the desired NTP Client poll rate. Sentinel allows poll rates from 1 per second to 1 per 36.4 hours. If the rate chosen is greater than the NTP Server can accept then Sentinel will back the rate off, if requested, until it is acceptable to the NTP Server.

Ensure **Normalize delays** is set to **On**.

In monitor mode the NTP Server / Client pair to be monitored can be configured on the **Settings > Monitored Channels > Monitor Mode** page. This can be configured manually or the **Discover** function used. Pressing the **Discover** button will bring up a pop-up box with a list of all NTP flows detected. Selecting the appropriate flow will cause the **Monitored Server IP** and **Monitored Client IP** boxes to be automatically populated.

Ensure **Normalize delays** is set to **On**.

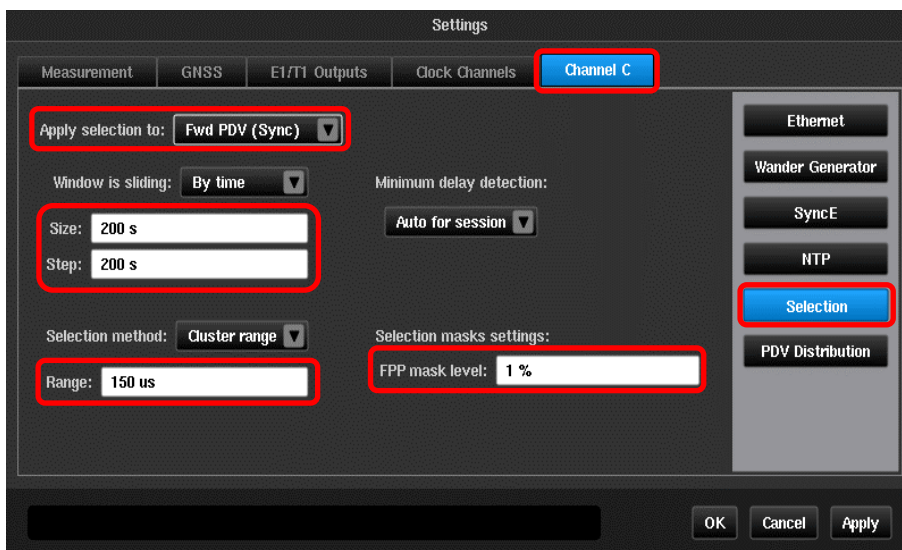


NOTE: For low poll rates Sentinel may not discover any NTP flows and the settings should be manually entered.

3.6 Packet Selection for FPP Measurements to G.8261.1

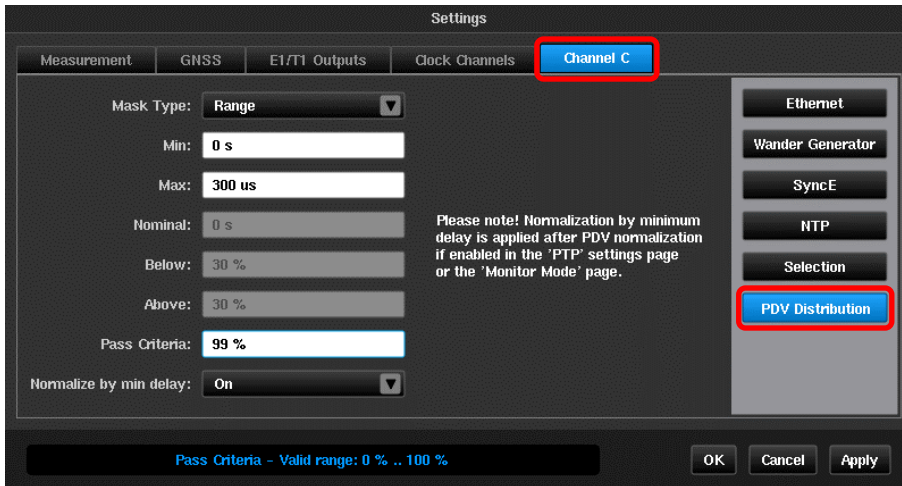
From the **Settings > Channel x > Selection** or **Settings > Monitored Channels > Selection** page, configure the packet selection parameters as follows.

1. Select **Fwd PDV (Sync)** from the **Apply selection to** dropdown box.
2. Set the parameters for packet selection.
3. Set Pass/Fail **FPP mask level** to 1% for FPP analysis. Please refer to appendix C for definition of FPP.



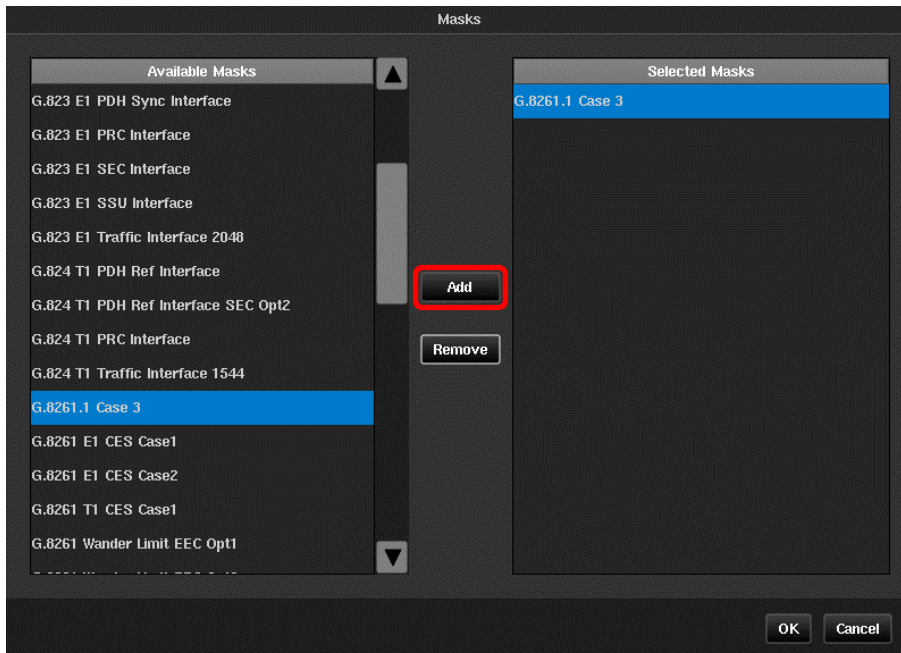
3.7 Vendor Specific Network PDV Distribution (PDD) Pass/Fail Criteria

Configure Pass/Fail criteria for Packet Delay Distribution (PDD) analysis on the **Settings > Channel x > PDV Distribution** or **Settings > Monitored Channels > PDV Distribution** page. This Pass/Fail criterion is vendor specific. Please consult vendor for parameters. If vendor has no spec for network PDV, then there is no need to configure this page.



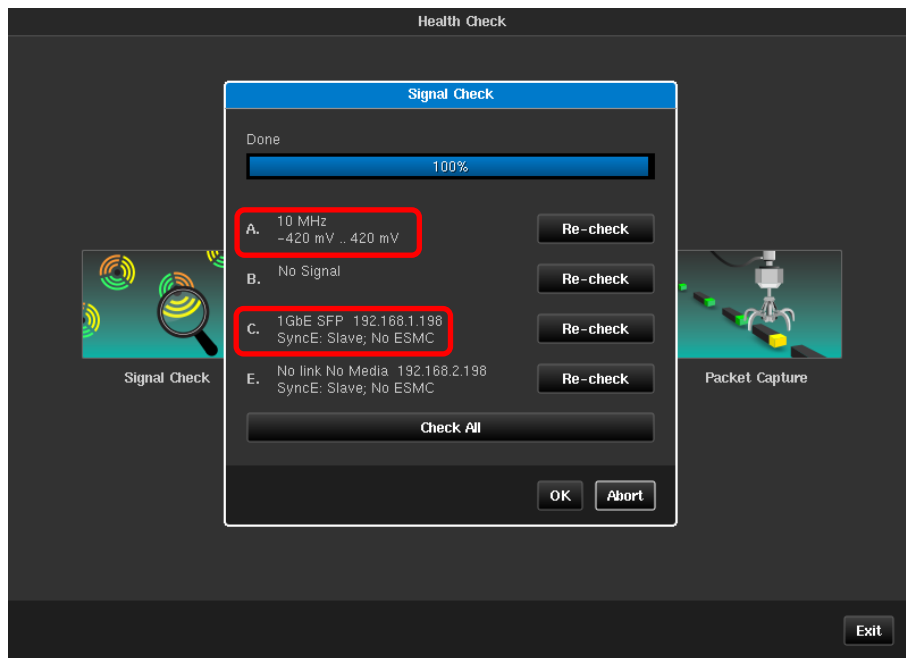
3.8 Select Recovered Clock Mask

Select packet metrics related masks from the **Masks** tab. Mask G.8261.1 Case 3 is recommended for network conformance test. This mask is explained in Appendix D.



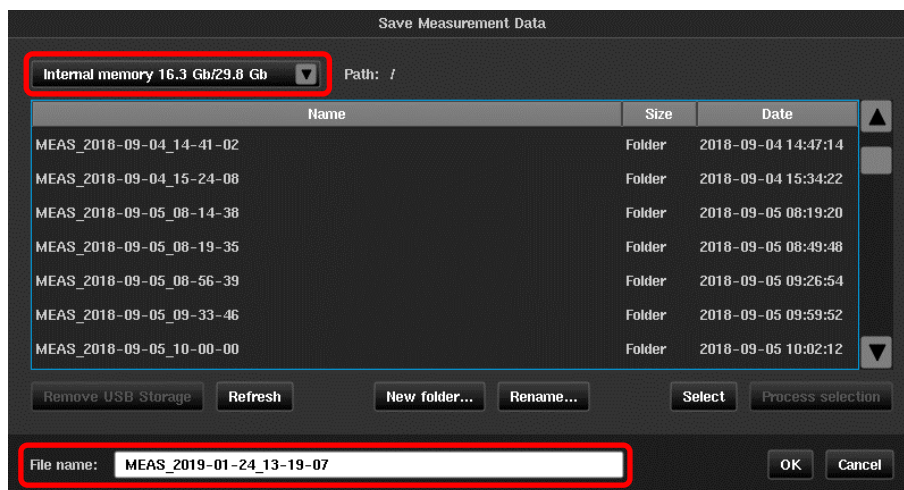
3.9 Signal Check

1. Click on the **Health Check > Signal Check** button.
2. Make sure the signal check is successful and as expected. An example screen shot is shown below.



3.10 Start the Test

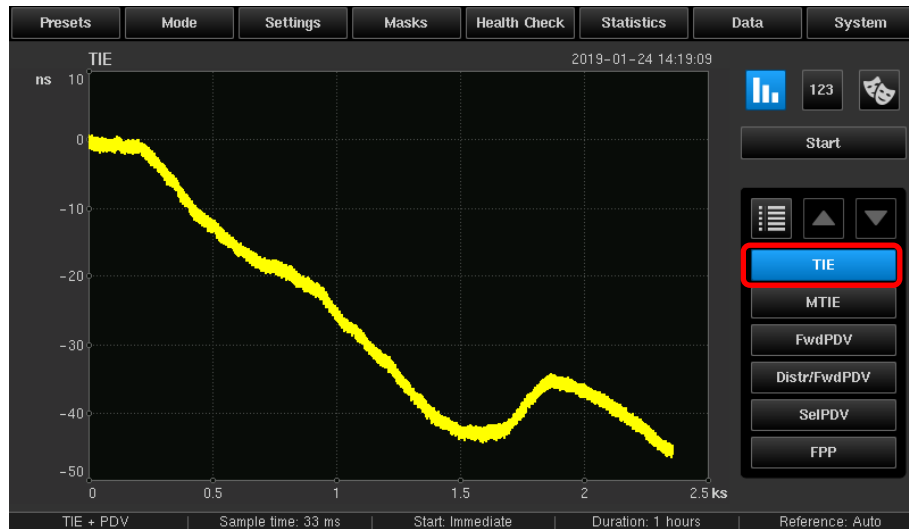
1. Click on the "Start" button.
2. Sentinel will prompt you to select where to store the measurement results. The results can be either saved on Sentinel internal memory or external USB stick.



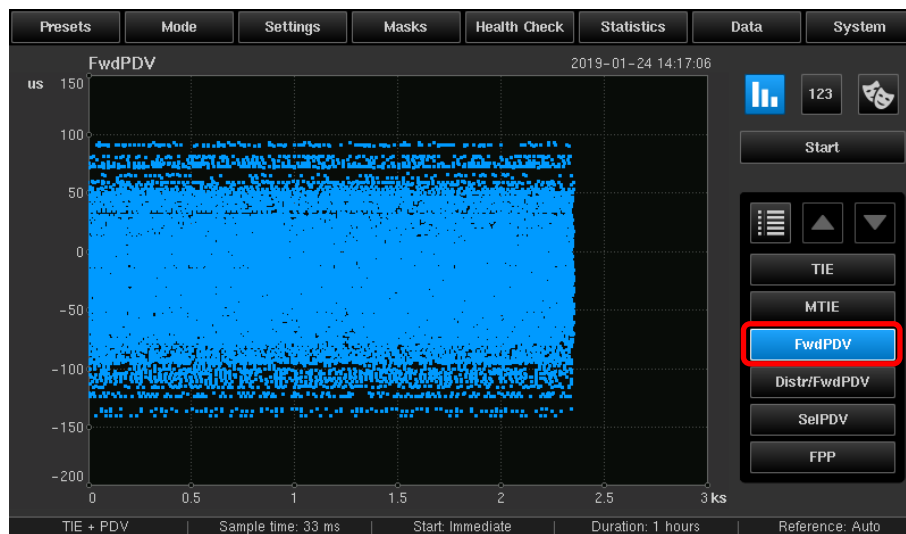
NOTE: For longer term measurements, it is always recommended to use an external USB memory stick to ensure sufficient storage space.

4 Measurement Results Display

Once the measurement starts, the TIE graph of recovered clock will be displayed on the main GUI window as the following graph.



The PDV for forward direction (from NTP Server > NTP Client) is also graphed. To view PDV for forward direction, click on the **Fwd PDV** button.



NOTE: Sentinel also graphs the PDV for the reverse direction (NTP Client > NTP Server). If **Normalize delays** is set to **Off**, Sentinel can also calculate Path Delay and 2Way Time Error. These metrics may be of interest where NTP is used to define time and phase but are not required or quantified for frequency synchronization.

5 Test Cases

Test case 5.1 evaluates the performance of the network against vendor specific limits. Test Cases 5.2 and 5.3 evaluate the performance of the network and the recovered clock against the ITU-T G.8261.1 recommendation. Test case 5.4 provides further troubleshooting and debugging information to perform further analysis on the results of 5.1, 5.2 and 5.3.

Note: All test cases can run simultaneously, i.e. ONE single test.

5.1 Packet Delay Distribution (PDD) Analysis

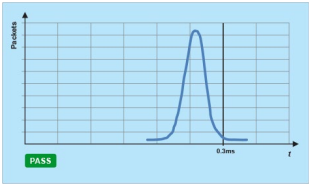
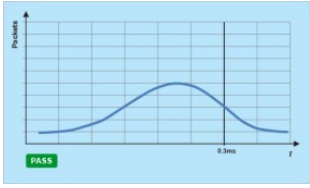
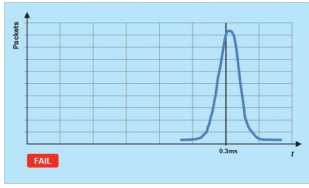
Performing PDD function analysis is important for many vendor's NodeB equipments. Many NodeB equipments (Ericsson RBS for example) have a specification where the distribution of the packets should meet particular limits.


5.1.1 Analyze and View PDD

To analyze PDD on Sentinel, select **Distr/FwdPDV** from the metric menu.



5.1.2 Sample PDD Test Results

Example Results			
	Within PDD limits - Pass	PDD close to limits	PDD outside limits - Fail
Possible Causes	n/a	<ul style="list-style-type: none"> • QoS Priority setting in the network is wrong • Network congestion • Re-route event 	<ul style="list-style-type: none"> • QoS Priority setting in the network is wrong • Network congestion • Re-route event
Possible Impact	n/a	<ul style="list-style-type: none"> • Congestion causes depopulation of the floor delay • Re-routes move the floor, reducing “headroom” for the PDD analysis. 	<ul style="list-style-type: none"> • Congestion causes depopulation of the floor delay. • Re-routes move the floor, eliminating all packets within the cluster range.
Next Action	n/a	<ul style="list-style-type: none"> • Visual inspection for re-routes and/or congestion. • If re-route event occurs, segment the data into separate data sets. • Apply PDD analysis separately to each data set. • If congestion, check NTP running at highest priority. • Check for over-subscription of allocated data rate. 	<ul style="list-style-type: none"> • Visual inspection for re-routes and/or congestion. • If re-route event occurs, segment the data into separate data sets. • Apply PDD analysis separately to each data set. • If congestion, check NTP running at highest priority. • Check for over-subscription of allocated data rate.

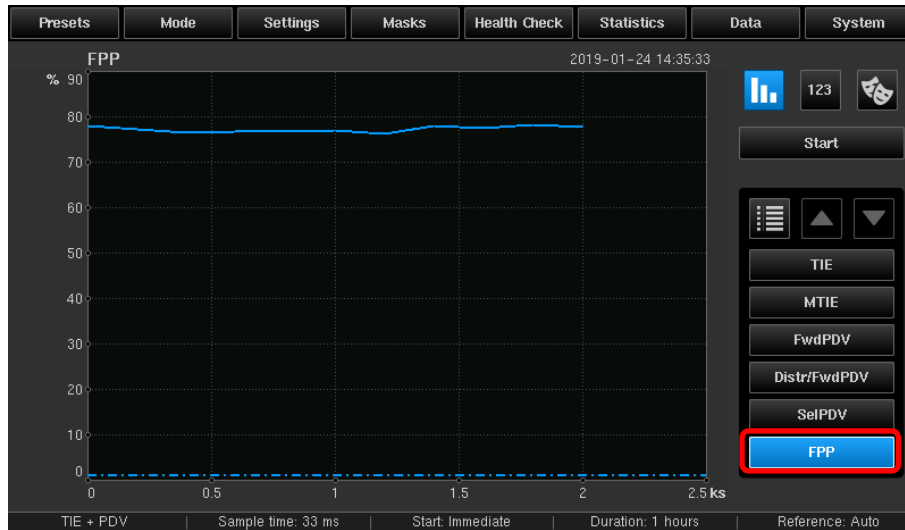
 **Note:** Consult each vendor for their specific Pass/Fail PDD limits. These limits may not be available from the standards.

5.2 Network PDV to ITU-T G.8261.1


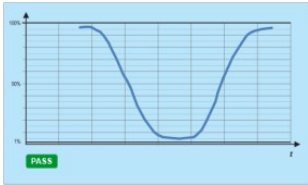
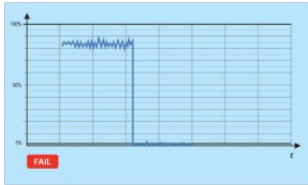
The Floor Packet Percent (FPP) metric is specified in ITU-T G.8260 to be used to evaluate the Network PDV. Pass/Fail evaluation is compared against the limit specified in ITU-T G.8261.1. Please refer to the Appendix for more information.

5.2.1 FPP Measurement and Analysis

To view FPP, click on the **FPP** button on the metrics menu. The Pass/Fail mask and the FPP graph will be displayed in the same window. The test fails if the FPP value ever falls below the mask.



5.2.2 Sample FPP Test Results

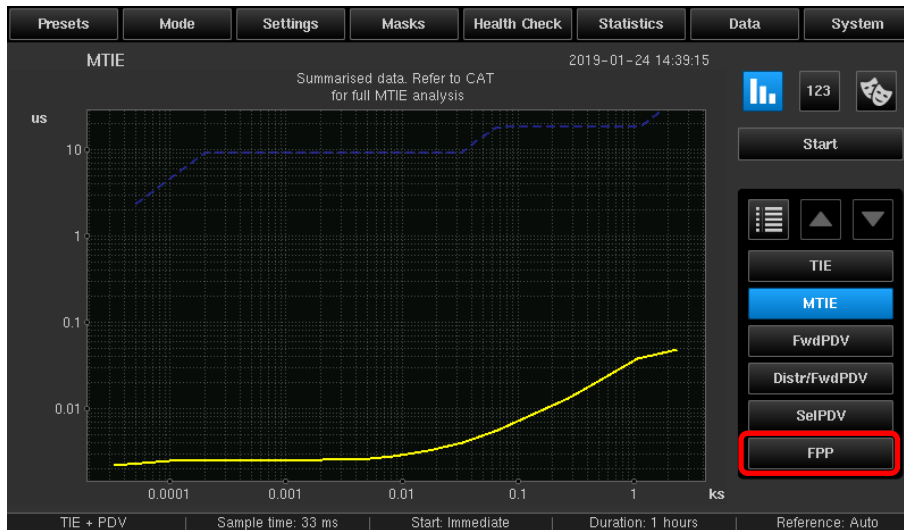
Example Results			
	Within FPP limits - Pass	FPP close to limits	FPP outside limits - Fail
Possible Causes	n/a	<ul style="list-style-type: none"> Priority setting wrong Network Congestion Re-route event 	<ul style="list-style-type: none"> Priority setting wrong Network Congestion Re-route event
Possible Impact	n/a	<ul style="list-style-type: none"> Congestion causes depopulation of the floor delay Re-routes move the floor, reducing "headroom" for the FPP analysis 	<ul style="list-style-type: none"> Congestion causes depopulation of the floor delay Re-routes move the floor, eliminating all packets within the cluster range
Next Action	n/a	<ul style="list-style-type: none"> Visual inspection for re-routes and/or congestion 	<ul style="list-style-type: none"> Visual inspection for re-routes and/or congestion

		<ul style="list-style-type: none"> • If re-route event occurs, segment the data into separate data sets • Apply FPP analysis separately to each data set • If congestion, check NTP running at highest priority • Check for over-subscription of allocated data rate 	<ul style="list-style-type: none"> • If re-route event occurs, segment the data into separate data sets • Apply FPP analysis separately to each data set. • If congestion, check NTP running at highest priority • Check for over-subscription of allocated data rate
--	--	--	---

5.3 Recovered Clock Stability to ITU-T G.8261.1³

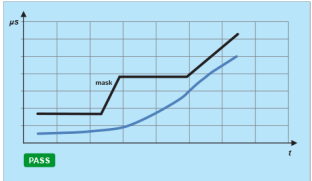
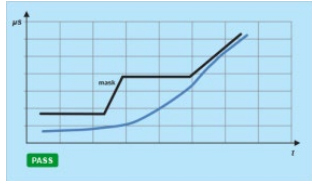
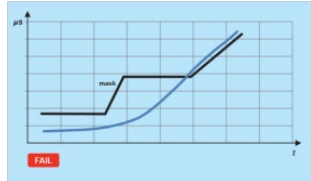
5.3.1 Compare with MTIE Mask

To view MTIE and compare with the mask, click on the **MTIE** button. The G.8261.1 mask will also appear in the same display area as a dashed line. Multiple masks can be selected at the same time for comparison. The screenshot shows recovered clock wander measurement. The test passes if the clock MTIE is always below the mask.



³ ITU-T G.8261.1 specifies the wander limit at the clock out interface of a NTP client

5.3.2 Sample G.8261.1 Test Results

Example Results			
	Within G.8261.1 limits	Close to G.8261.1 limits	Outside G.8261.1 limits
Possible Causes	n/a	<ul style="list-style-type: none"> The network PDV is stressing the slave to its limit with the current network configuration Network equipment failure 	<ul style="list-style-type: none"> The network PDV is too stressful for the client The priority setting for NTP packets may be too low The traffic level in the network may be too high Temperature variable may be too high which impacts the performance of clocks
Possible Impact	n/a	<ul style="list-style-type: none"> Interference at air interface Drop calls Handover failure Slow data transmission 	<ul style="list-style-type: none"> Interference at air interface Drop calls Handover failure Slow data transmission
Next Action	n/a	<ul style="list-style-type: none"> Share the PDV Capture with NTP Client vendor (and NodeB vendor if external Client is used) Replay the PDV in the lab to troubleshoot and adjust Client algorithm to increase margin Look at re-routes and re-engineering the network to reduce PDV stress Re-test 	<ul style="list-style-type: none"> Share the PDV Capture with NTP Client vendor (and NodeB vendor if external Client is used) Replay the PDV in the lab to troubleshoot and adjust Client algorithm to enable it to pass mask Look at re-routes and re-engineering the network to reduce PDV stress Re-test

5.4 NTP Packet to Packet PDV Capture

The NTP PDV graph gives information such as:

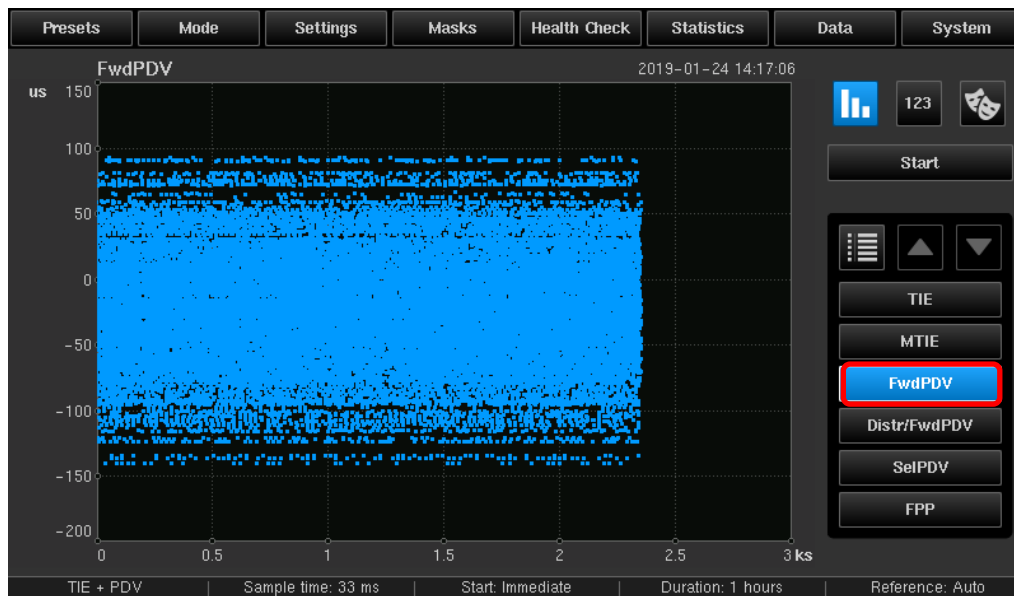
- Average/standard deviation of PDV
- Delay jumps due to routing changes or dramatic traffic changes.

From the PDV graphs, post-analysis can be performed on the data such as packet metrics.

NOTE: These PDV files can be sent back to the operator's lab or the vendor's R&D center to reproduce the issues seen with Sentinel and take remedial action.

5.4.1 View PDV Graph

To view the PDV graphs, select **Fwd PDV** from the metric menu.



6 Test Results Interpretation

6.1 With Client Clock Output

Clock Output (5.3) Network PDV (5.1, 5.2)	Pass	Fail
Pass	OK	Contact NTP Client vendor * Please refer to the "next action" in section 5.3
Fail	Network PDV is high but NTP Client can work OK with it **	Network re-route or re-engineer may be required. Please refer to the "next action" in sections 5.1, 5.2 and 5.3

* Network PDV has been deemed to meet FPP limits and vendor specific PDD limit. Network PDV packet-to-packet capture should also be analyzed and sent to the NTP Client vendor to allow troubleshooting.

** Although the PDV is OK for this NTP client, any software update to the Client or using a different NTP Client in the network, may cause a failure. It is advised that further testing is performed to validate the client's performance.

6.2 Without Client Clock Output

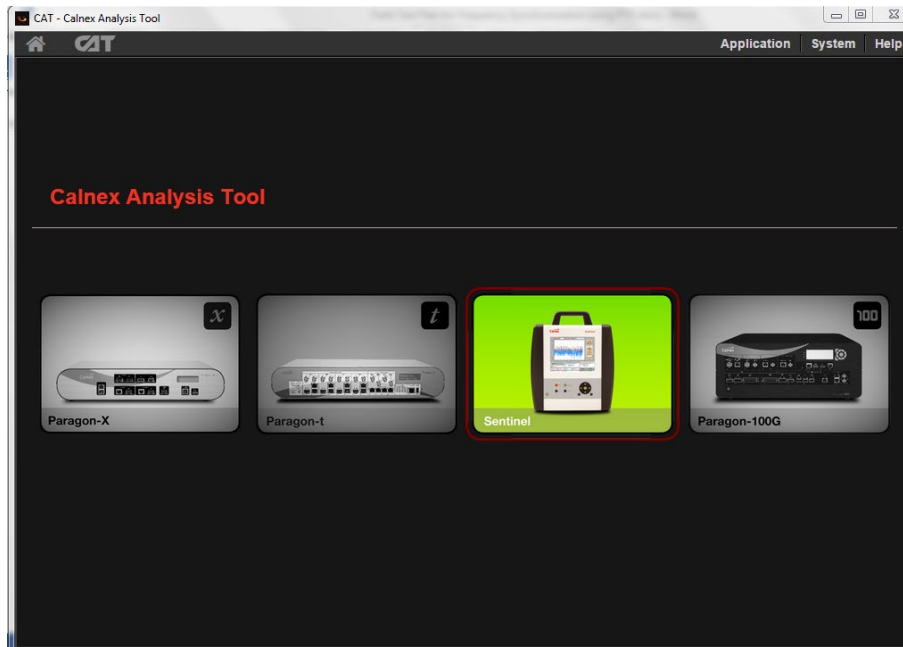
In case of no clock output from the client, always check the measurement results from section 5.1, 5.2 and 5.4 for further actions.

NOTE: This test procedure focuses on frequency synchronization using NTP. Please refer to other test documents from Calnex for frequency synchronization test and synchronization test for TDD-LTE using PTP.⁴

⁴ Calnex document number CX5019

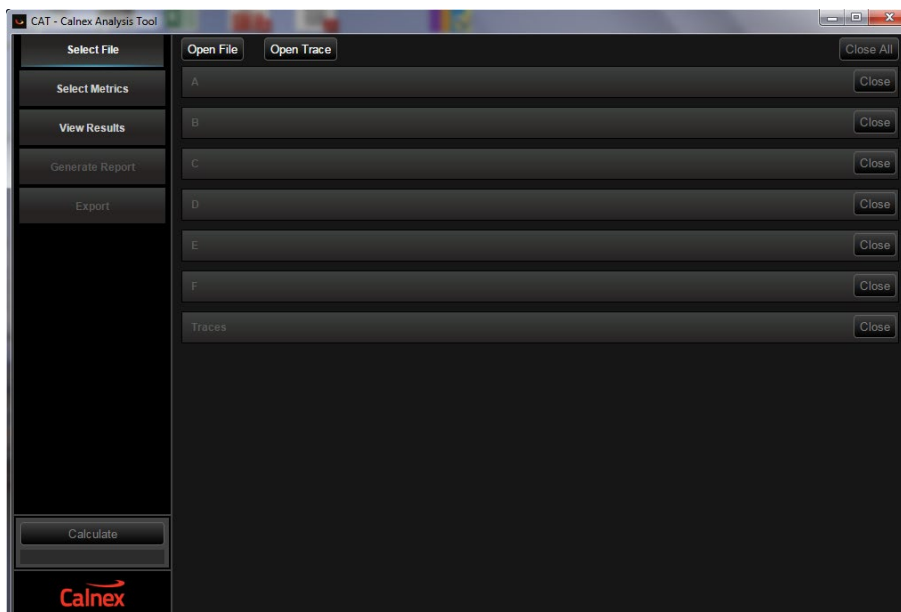
7 Offline Analysis and Report Generation using CAT

The Calnex Analysis Tool (CAT) is a standalone software tool⁵ for MTIE/TDEV, MAFE, FPP and PDD analysis with integrated pass/fail masks. The captured raw data from Sentinel can be imported to CAT for such metric analysis. More importantly, professional reports can be easily generated with a single click from CAT.



7.1 Import Results

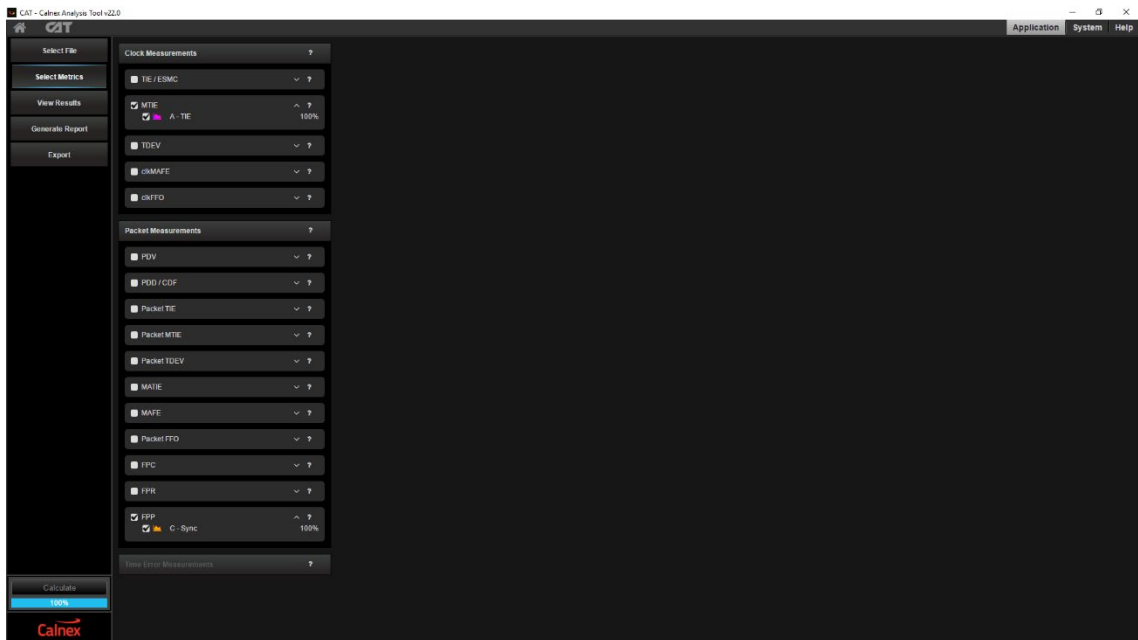
To import data from Sentinel to CAT, from the CAT GUI interface, select **Application > Select File > Open File** or select and drag Sentinel .dset files from file explorer to the CAT GUI. Multiple files can be imported at the same time.



⁵ Included with Sentinel

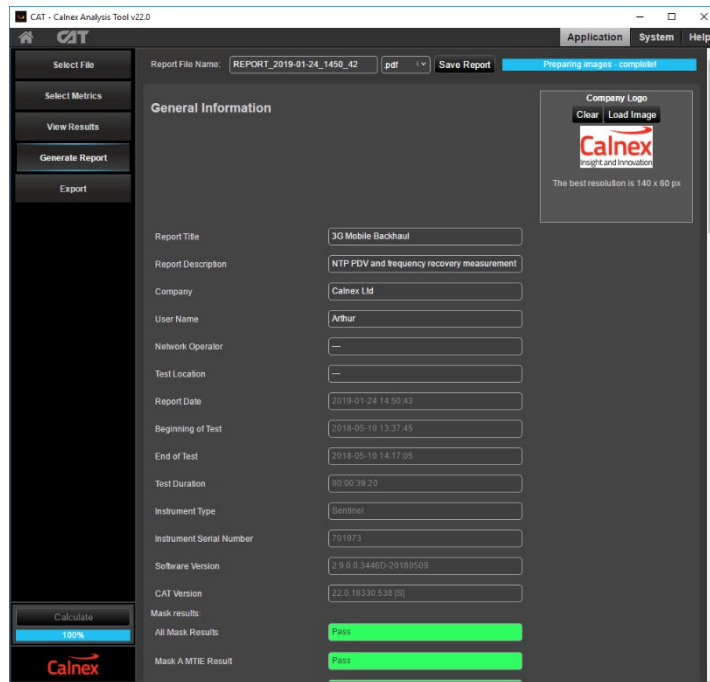
7.2 Select Metrics

The appropriate tick box can be selected from the “Measurement Analysis” menu for required metrics analysis after the measurement files have been imported.



7.3 Generate a Report

To generate a professional report⁶, simply click on **Generate Report** from CAT GUI.



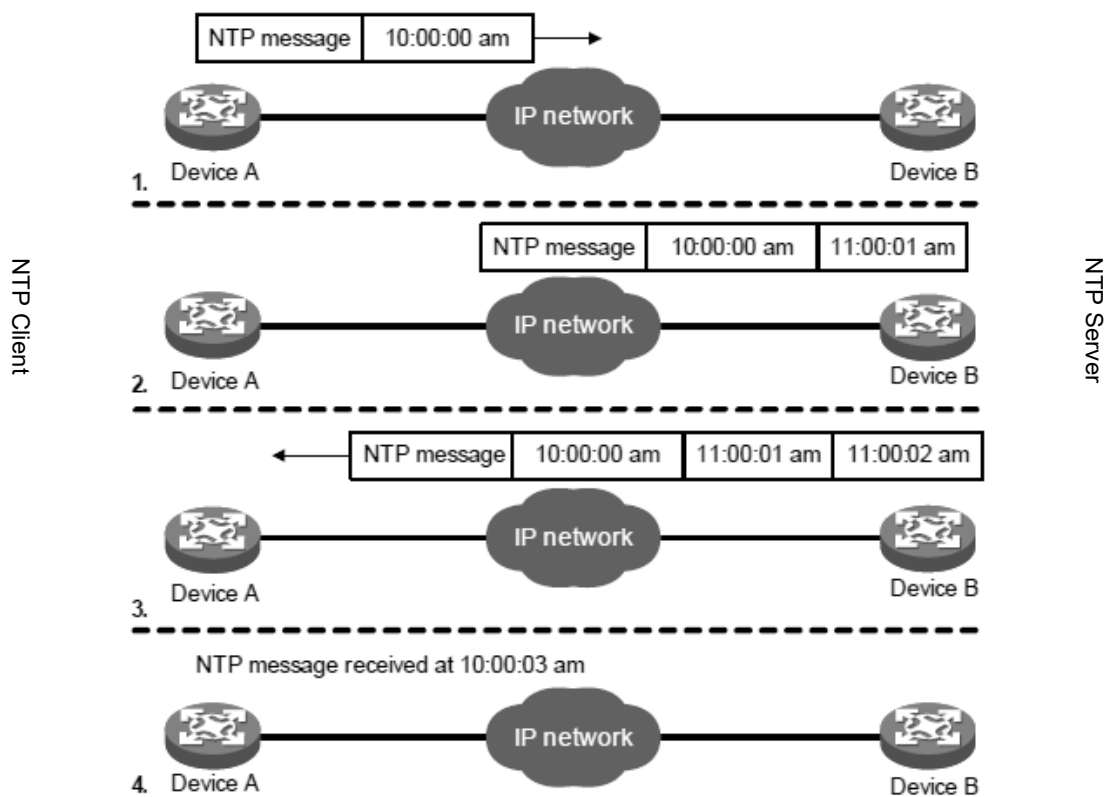
⁶ See Appendix E for example report

Appendix A: NTP Synchronization Technology

This section explains how NTP as a protocol works. This is the same mechanism for NTPv3 and NTPv4. The diagram shows the basic work flow of NTP. Device A and Device B are interconnected over a network. They have their own independent system clocks, which need to be automatically synchronized through NTP.

For an easy understanding, we assume that:

- Prior to system clock synchronization between Device A and Device B, the clock of Device A is set to 10:00:00 am while that of Device B is set to 11:00:00 am.
- Device B is used as the NTP time server, namely Device A synchronizes its clock to that of Device B.
- It takes 1 second for an NTP message to travel from one device to the other.



The process of system clock synchronization is as follows:

1. Device A sends Device B an NTP message, which is time stamped when it leaves Device A. The time stamp is 10:00:00 am (T1).
2. When this NTP message arrives at Device B, it is time stamped by Device B. The timestamp is 11:00:01 am (T2).
3. When the NTP message leaves Device B, Device B timestamps it. The timestamp is 11:00:02 am (T3).
4. When Device A receives the NTP message, the local time of Device A is 10:00:03 am (T4).

Up to now, Device A has sufficient information to calculate the following two important parameters:

1. The roundtrip delay of NTP message: $\text{Delay} = (T_4 - T_1) - (T_3 - T_2) = 2 \text{ seconds.}$
2. Time difference between Device A and Device B: $\text{Offset} = ((T_2 - T_1) + (T_3 - T_4))/2 = 1 \text{ hour.}$

Based on these parameters, Device A can synchronize its own clock to the clock of Device B. This is only a rough description of the work mechanism of NTP. For details, refer to RFC 1305.

This mechanism is extremely similar to PTP with two noticeable differences:

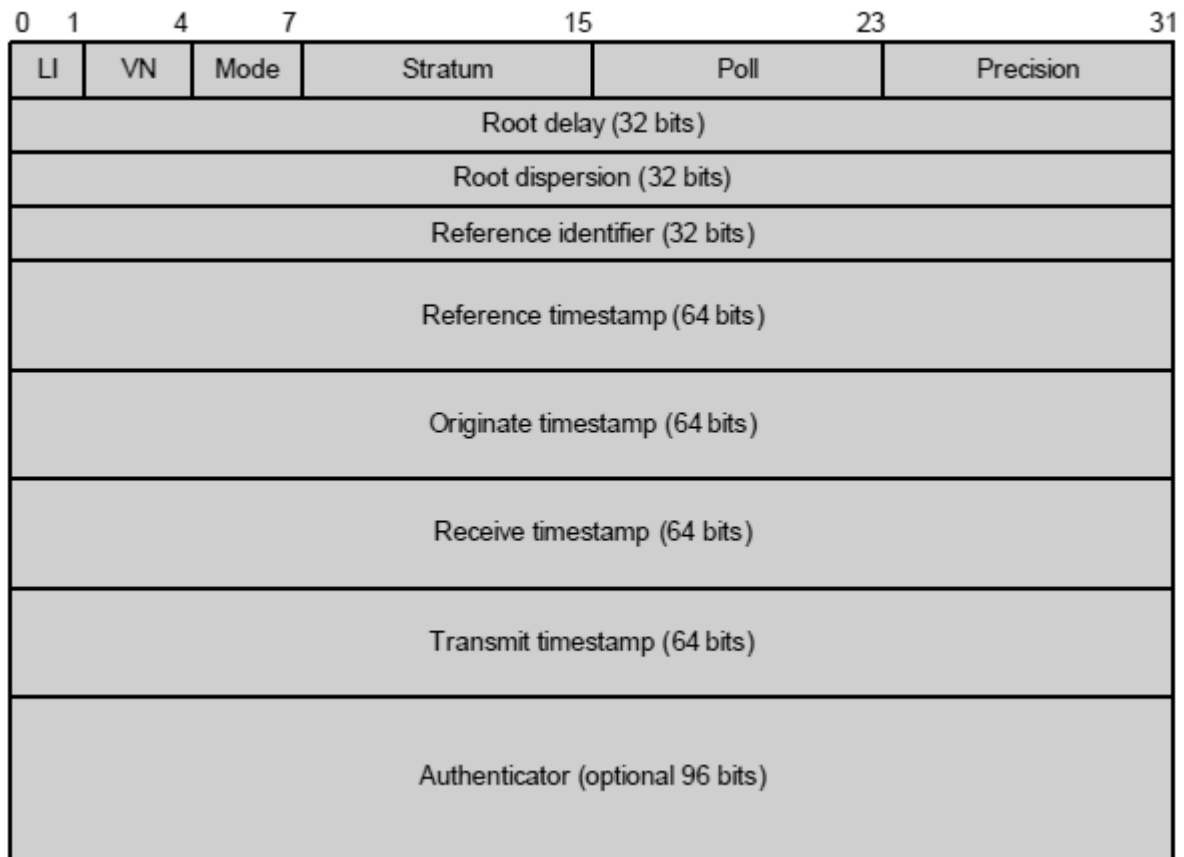
1. NTP Client initiates the message exchange instead of the NTP server. For PTP, the Grandmaster (Server) initiates the message exchange.
2. Each NTP message contains multiple timestamps. For PTP, a message can only contain one timestamp. In some cases, the message may not contain any timestamp (i.e. Delay Request).

Whether it is NTP or PTP, the client or slave requires T_1 , T_2 , T_3 and T_4 to work out the round trip delay and the client/slave error in order to be time synchronized.

For completeness, the NTP message header is shown. The explanations of the timestamps are as follows:

1. Reference Timestamp: the local time at which the local clock was last set or corrected.
2. Originate Timestamp (T_1): the local time at which the request departed the client for the service host.
3. Receive Timestamp (T_2): the local time at which the request arrived at the service host.
4. Transmit Timestamp (T_3): the local time at which the reply departed the service host for the client.

NOTE: T_4 is when the client receives the 'server message', hence it will not be sent in a message to the server.



Some of the key reasons why only millisecond accuracy can be obtained by standard NTP are:

1. NTP only sends a timing packet once every 16 seconds (this is a maximum rate):

The large amount of time between packets means that the server time can 'wander' away from real time between packet arrivals.

Note: Some vendors may implement proprietary NTP which supports higher packet rate up to 1 packet per second.

2. NTP uses software timestamping:

Almost all NTP standard solutions use software timestamping of packet arrival and transmission events. Software timestamps are inherently inaccurate because they rely on the many variable factors within the computer that is running the NTP daemon. Issues such as IP stack delay, interrupts etc ensure that the timestamp cannot be accurate.

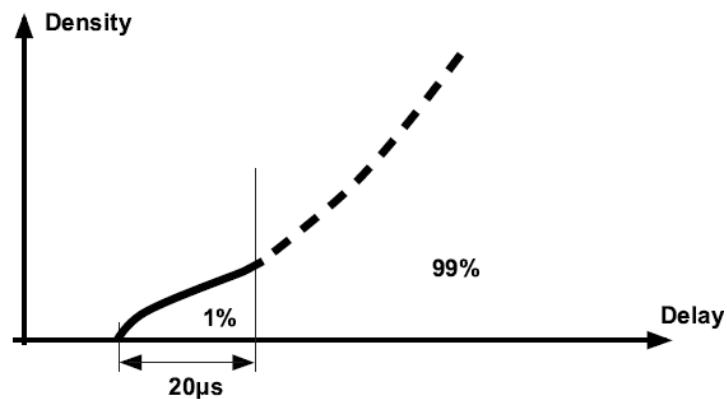
3. NTP uses a standard time recovery algorithm:

The time recovery algorithm has to take account of network jitter effects on the timing packets. It must effectively remove the network jitter to determine what the relationship of the time in the server to true time in the NTP master is. NTP defines this algorithm in the NTP standard. Whilst it is a perfectly acceptable algorithm for Wide Area time recovery to millisecond accuracy it is simply not intelligent enough to deliver time to a better accuracy than this.

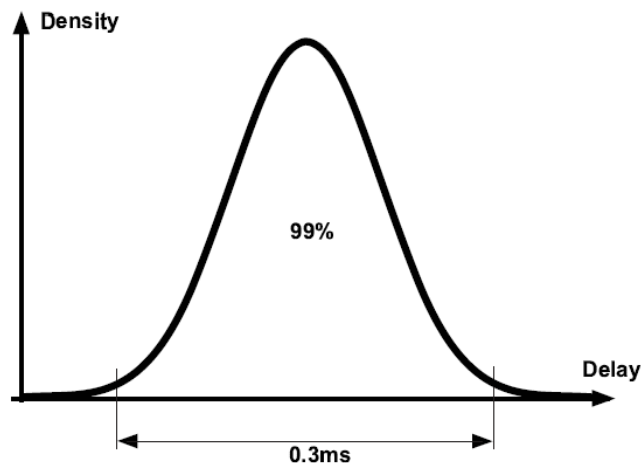
Appendix B: Example Ericsson RBS PDD limits

In order for Ericsson RBS NodeB to sync to the NTP Server in 16 minutes, the PDV for the NTP packets must meet either one of the following three conditions.

- PDV for the 1% packets having the lowest delay is maximum 20 μs during 16 minutes period as shown below.



- The interface characteristics comply with the tolerance for IP synchronization references in G.8261 test case 12 to 17 in G.8261 Appendix VI.5.2 with traffic model 2 according to G.8261 Appendix VI.2.2
- PDV has an approximately time invariant Gaussian distribution with PDV for 99% of the packets of maximum 0.3ms as shown below.



Therefore, it is very important to analyse the PDV distribution characteristic of the ingress NTP packets to the Ericsson NodeB to ensure the requirements are met. Otherwise, it may take much longer to lock, or even prohibit locking.

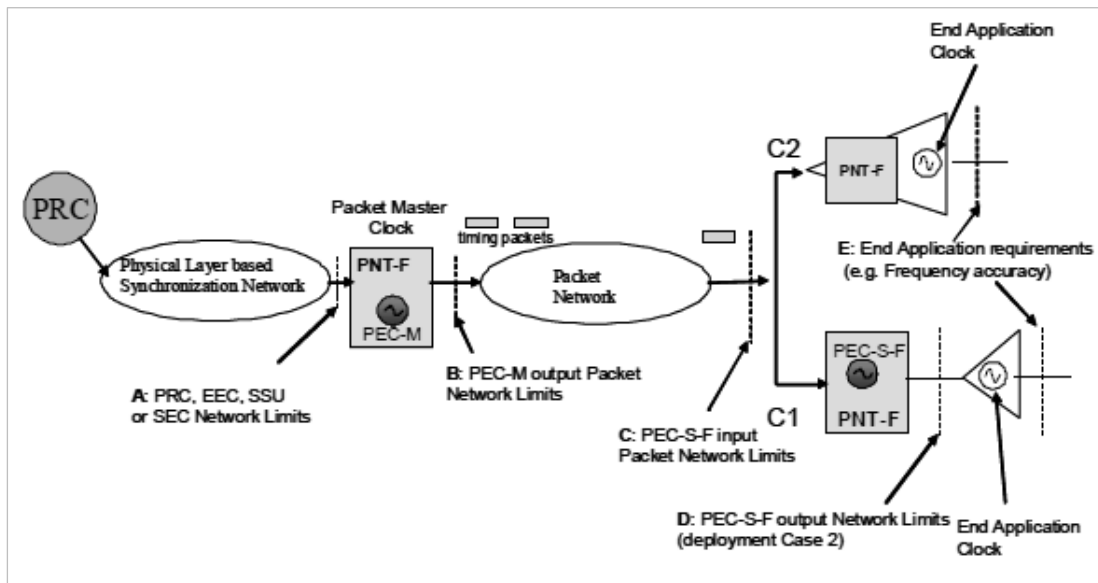
Among these three criteria, criteria #2 is to test the tolerance of the interface in the presence of various traffic models defined in ITU-T G.8261 test case 12-17. This test should be performed before any equipment is deployed in the network.

Appendix C: ITU-T Recommended Network Limits for Packet Networks

Floor Packet Percent (FPP) by definition is the percentage of packets that fall into the given fixed cluster range starting at the observed floor delay. FPP are applicable to defining the network limits.

Network Limits

ITU-T G.8261.1 defines different levels of reference points and their network limits in packet networks for frequency synchronization as follows.



Network limits are specified at different levels of reference points. At reference point C, the packet network limits are expressed in terms of the relevant PDV based metric called **FPP (Floor Packet Percentage)** as follows:

With window interval $W = 200s$ and fixed cluster range $\delta = 150\mu s$ starting at the floor delay, the network transfer characteristic quantifying the proportion of delivered packets that meet the delay criterion should satisfy

$$FPP(n, W, \delta) \geq 1\%$$

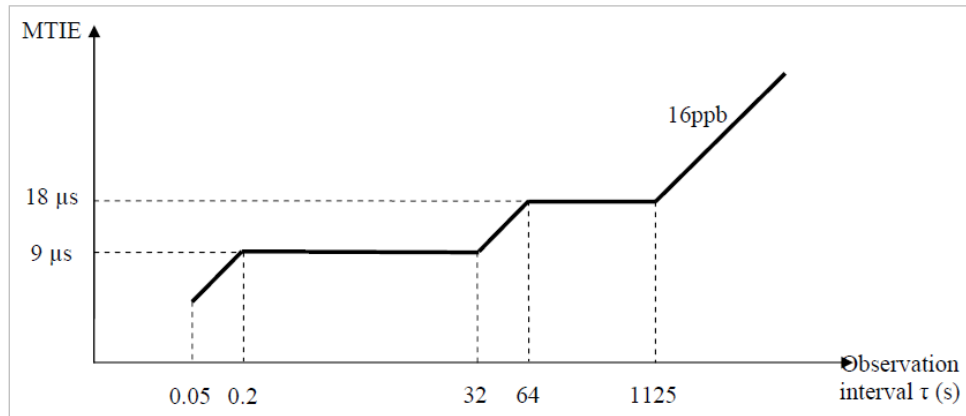
That is the floor packet percentage must exceed 1%.

Conformance test to FPP is mentioned in this document as test procedure 5.2.


Appendix D: ITU-T Recommended Client Clock Network Limits

Per the above network reference model, ITU-T also defines the network limit in terms of frequency wander at reference point D. This is to measure the accuracy or wander of the recovered Client clock normally done at the frequency output interface on Client (NodeB), such as 2MHz, 2Mbits or 10MHz.

The output wander network limit applicable at reference point D is provided by the graph below. It is in terms of MTIE. This is discussed in section 5.3 in this document.



Appendix E: Example Generated Report



General Information

Report Title	3G Mobile Backhaul
Report Description	NTP-PDV and frequency recovery measurement
Company	Calnex Ltd
User Name	Arthur
Network Operator	---
Test Location	---
Report Date	2016-05-24 14:50:43
Beginning of Test	2016-05-10 13:37:45
End of Test	2016-05-10 14:17:05
Test Duration	00:00:39.20
Instrument Type	Sentinel
Instrument Serial Number	701973
Software Version	2.9.0.0.34460-20160509
CA T Version	22.0.18330.538 [S]

Mask results:

All Mask Results	Pass
Mask A MTIE Result	Pass
Mask C FPP Result	Pass

Instrument Test Configuration

Frequency Reference Source	Internal - Rb
----------------------------	---------------

Channel A Test Configuration


Network / Device Under Test	
TIE Sample Rate	0.033

Channel C Test Configuration


Network / Device Under Test	
Physical Medium/Line Rate	1GbE SFP
Encapsulation	UDP/Pv4
Sync Pkt Rate	16
Delay Req Pkt Rate	16
Master Address	192.168.1.11
Slave Address	192.168.1.198
Domain	4
VLAN Id	
Two-Step	True
Unicast / Multicast	Unicast

Master Information


gmIdentity	00000E0F0E010A0D
gmClockQuality.clockClass	84
gmClockQuality.clockAccuracy	100ns
gmClockQuality.osrv	0x6400
gmPriority1	128
gmPriority2	128




Page 1 of 4



currentUtcOffset	37
stepsRemoved	0
timeSource	GPS



Page 2 of 4

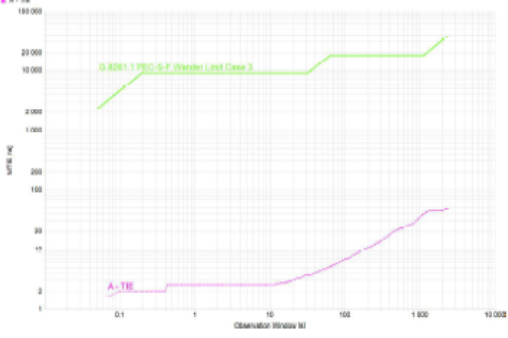


Results


TIE Measurement

Channel	A
Description	
Physical Medium	
Line Rate	
Measurement Start	2016-05-10 13:37:45
Measurement Stop	2016-05-10 14:17:05
Mask MTIE	G.8261.1 FEC-B4 Wander Limit Case 3
Mask MTIE Result	Pass


MTIE Analysis



Min [ns]	1,566
Max [ns]	47,094
Max-Min [ns]	45,528



Page 3 of 4

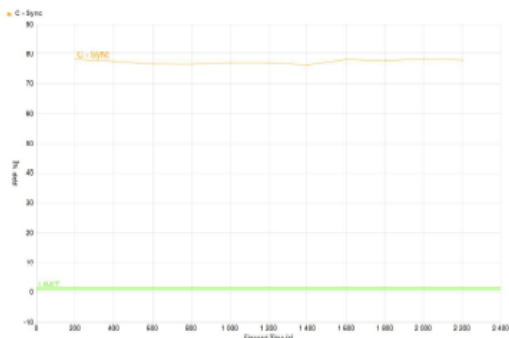



Sync Measurement

Channel	C
Description	
Physical Medium	
Line Rate	
Measurement Start	2016-05-10 13:37:45
Measurement Stop	2016-05-10 14:16:58

FPP Analysis

Direction	Forward
Window Size	200s
Window Step Size	200s
FloorDelta	150µs
Limit	1%
Result	Pass





Page 4 of 4

Calnex Solutions Ltd
Oracle Campus
Linlithgow
West Lothian EH49 7LR
United Kingdom

t: +44 (0) 1506 671 416
e: info@calnexsol.com

calnexsol.com

© Calnex Solutions Ltd, 2019
This document is subject to change without notice.

CX5017 v0.9 January 19

