Secure PTP - Protecting PTP with MACsec without losing accuracy

VITESSE®

Making next-generation networks a reality.

ITSF 2014
Thomas Joergensen
Vitesse Semiconductor

Security issues with PTP

- It is possible to “spoof time” and attack PTP if the PTP traffic is unencrypted/unprotected
- Small cells are often placed in areas that do not provide physical protection
- Enterprise femtocells may use an existing Ethernet network in the buildings for both user traffic and PTP timing
- PTP for frequency (G.8265.1) is often running inside tunnels (EVCs) along with the customer traffic and the customer traffic must be encrypted
- There is no standard security protocol specified for PTP
  - Annex K in IEEE1588-2008 is known to be flawed and will be deprecated in next revision of the standard
- Many government regulations require information to be encrypted
- 3GPP TS 33.320 requires that the time delivery to Home Node B must be delivered over a secure backhaul link.

IEEE1588

Time Security

Networks Operate on Precision

What if Network Time is Compromised?

Mobile Communications	• No access to network • Calls will drop • Poor coverage and throughput
Smart Energy	• Time errors can trigger faults in power grid
Financial / Trading	• Smart Order routing for large trades requiring simultaneous execution on multiple exchanges may not function properly

Low latency security in conjunction with nanosecond-level time stamp synchronization is critical to network infrastructure

What about IPsec?

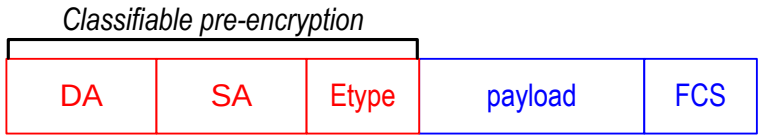
- **IPsec is sometimes used today to protect the mobile user traffic**
- **But…**
  - It can only protect IP traffic and G.8275.1 uses PTP over Ethernet directly
  - IPsec prevents the use of 1-step hardware timestamping as PTPoIP is in the IP payload
  - IPsec encryption/decryption at the end of the EVC creates very large Packet Delay Variation
    - PDV happens outside the EVC and thereby not part of the SLA for the EVC connection
    - Large PDV caused by IPsec decryption is preventing accurate timestamping after decryption

MACsec 101

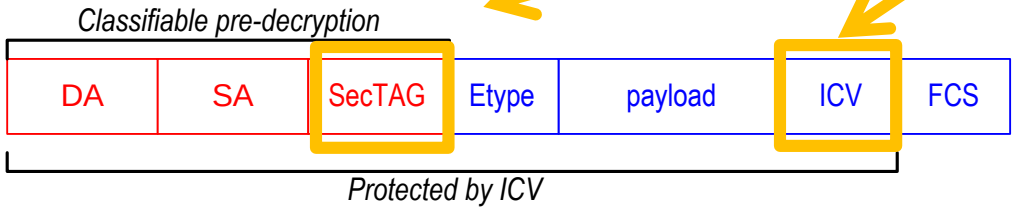
- MACsec is a layer 2 security protocol – IEEE802.1AE
- Provides strong 128/256bit encryption or protection with using the GCM-AES cipher suite
- Uses IEEE802.1X for authentication
- MACsec protects against
  - Passive wiretapping
  - Masquerading (MAC address spoofing)
  - Man-in-the-Middle attacks
  - Certain Denial-of-Service (DOS) attacks
- Designed for implementation in hardware (high bandwidth, low latency)
- Under consideration for next release of IEEE1588

MACsec Frame Format

Untagged Ethernet



Standard MACsec format

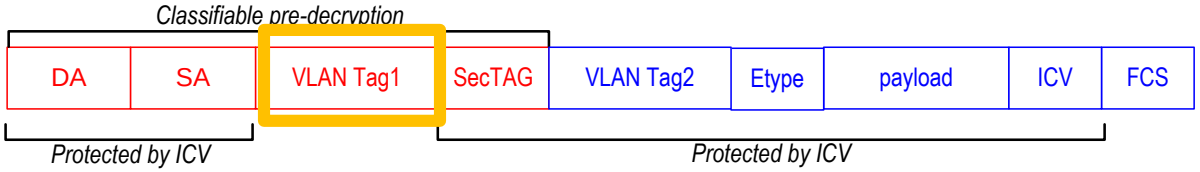


MACsec adds a SecTAG after the source address and an ICV field after the payload, protecting the complete frame

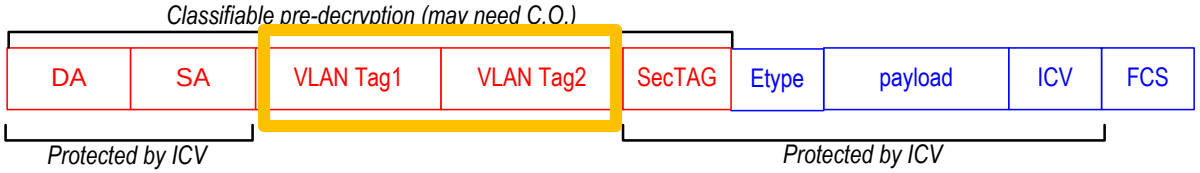
Provider Bridges can add/remove VLAN tags to the encrypted frame.

Some devices support bypassing existing VLAN tags when performing MACsec encryption/decryption

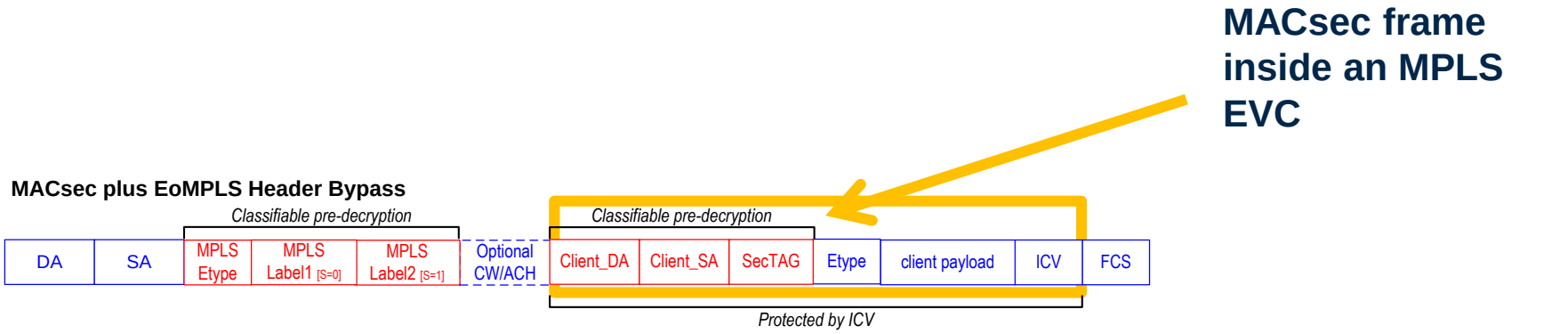
MACsec plus Single Tag Bypass



MACsec plus Dual Tag Bypass

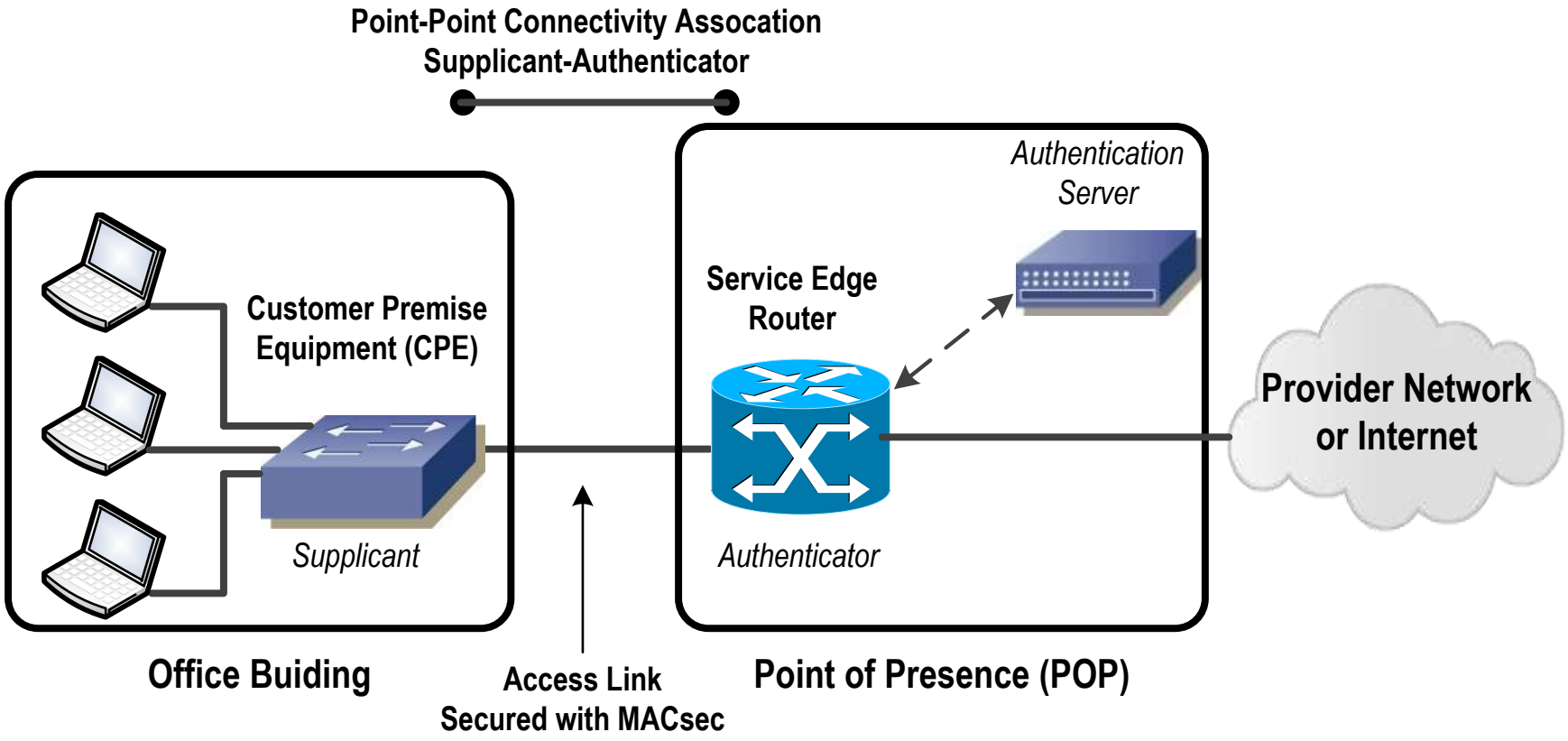


MACsec inside an MPLS EVC

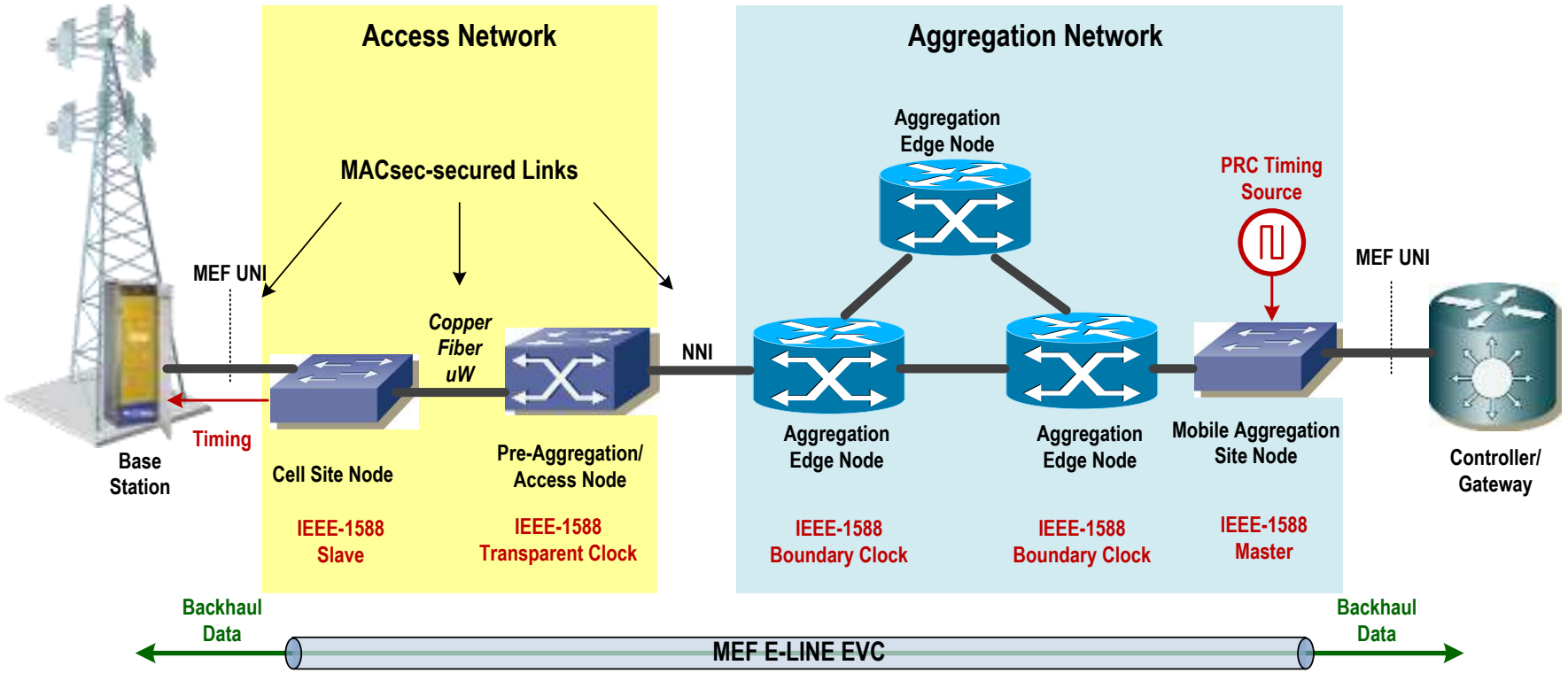


Protects MEF EVC payload while allowing network to push/pop VLAN tags and MPLS labels, as well as mark the frames for SLA-compliance (policing result)

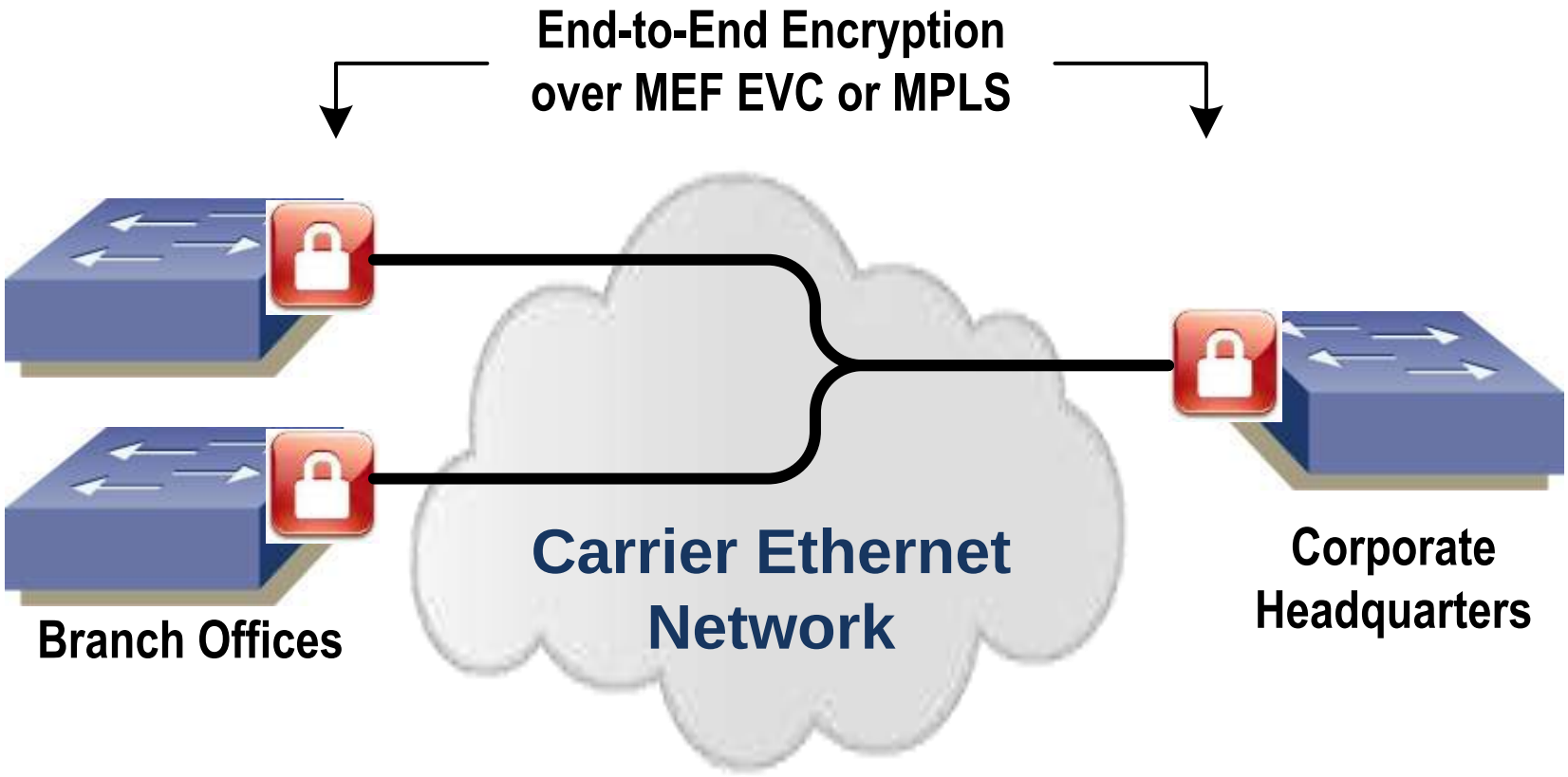
MACsec is normally point-to-point



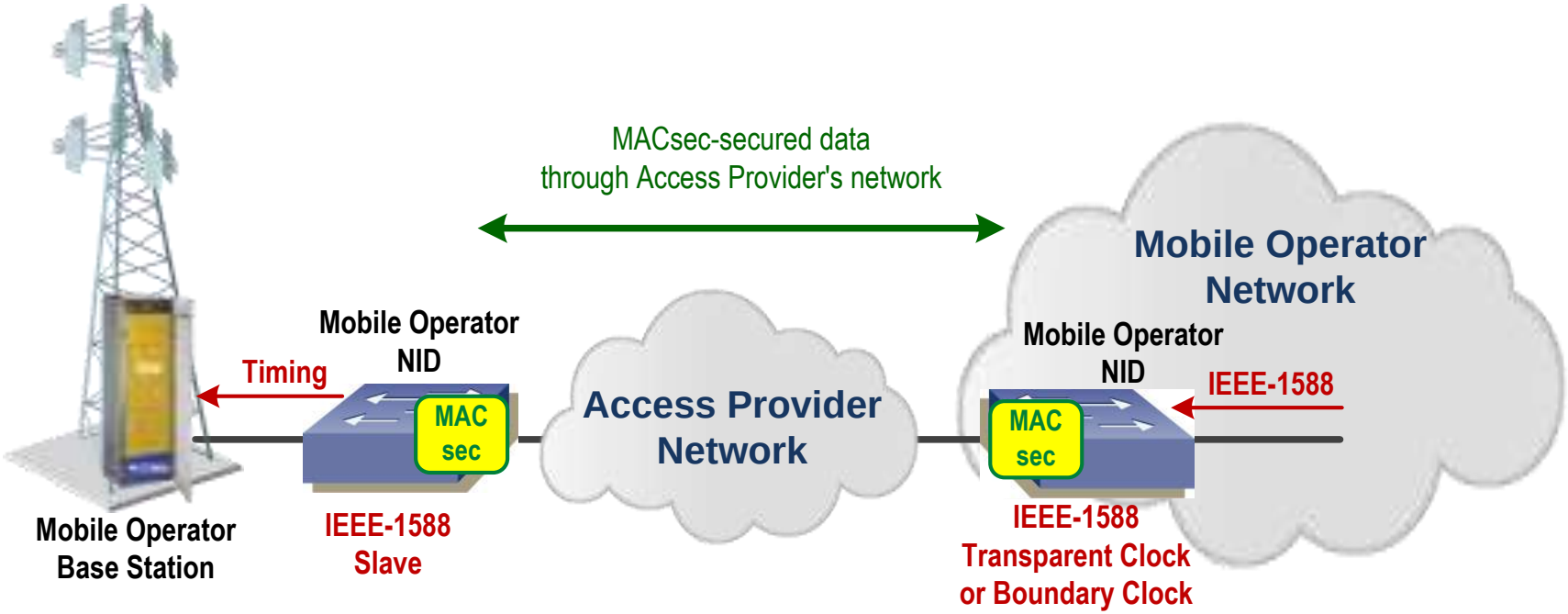
MACsec in Mobile Backhaul with IEEE-1588



MACsec can be used to protect EVCs



MACsec for EVC protection through access provider network



PTP phase over PTP-unaware/partially aware network – G.8275.2 (future)

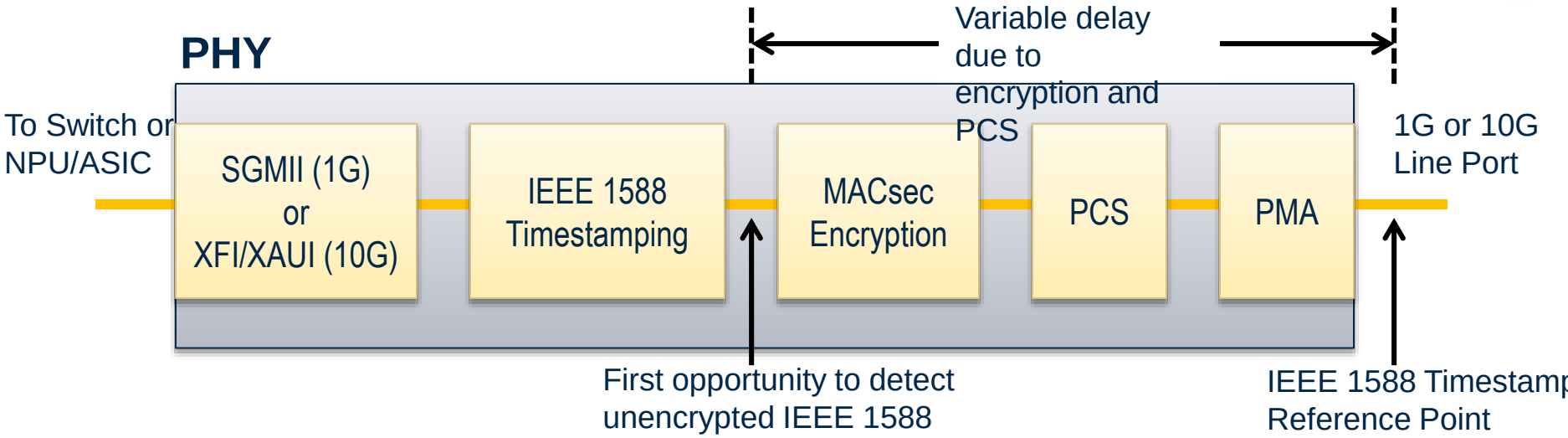
PTP frequency over PTP-unaware network – G.8265.1

Customer data can be protected using the same MACsec protected EVC

PTP and MACsec working together

- PTP-aware networks needs the ability to timestamp PTP frames on every port.
- MACsec protected networks encrypts/decrypts at the port/MAC
- By combining both functions in the same silicon it is possible to provide accurate timestamping of PTP frames
- Only solution to provide PTP 1-step operation
  - Significantly reduces the software load

Maintaining 1588 Accuracy with MACsec



- **MACsec processing introduces highly variable delays, standard MACsec destroys 1588 accuracy**
  - This is true even if 1588 remains unencrypted while other data is encrypted.
    Example: If the 1588 packet is immediately behind a packet that will be encrypted later, the encrypted packet grows by 24-32 bytes, delaying the 1588 packet by 192-256 ns compared to the case where the 1588 packet is behind a packet that won't be encrypted.

Test Results

VITESSE®

Making next-generation networks a reality.

VSC5621 Evaluation Board

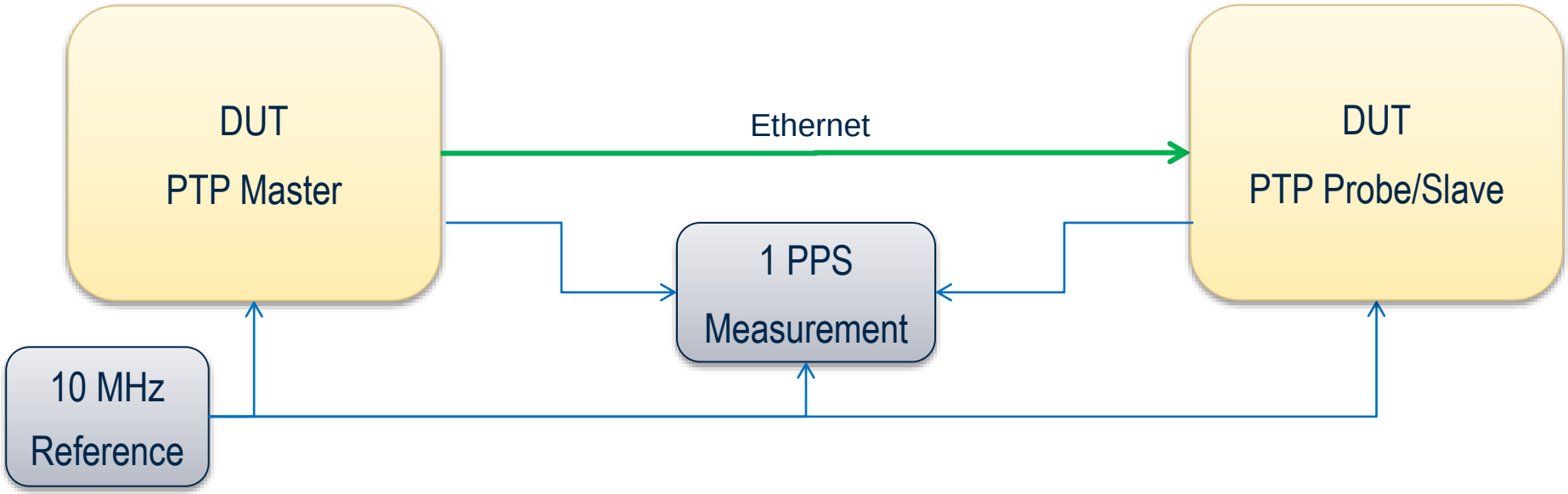
- **Complete Carrier Ethernet Switch with software**
  - Uses:
    - VSC7460 Carrier Ethernet Switch
    - VSC8584 Quad 1000BASE-T PHY with 1588 and MACsec
    - VSC8490 Dual 10G PHY with 1588 and MACSec
- **FIPS197 certified 256 bit MACsec solution**

FIPS CERTIFIED 197

intellisec

Test Setup –Timestamp Accuracy

- **PTP Master DUT and PTP Slave/Probe DUT is frequency locked to the same reference clock**
- **One DUT is configured in PTP probe (PTP slave) mode to measure received timestamp accuracy from PTP Master compared to the internal time in the DUT**
  - Test results will show the combined accuracy of the DUT probe (down to 1 ns depending on the DUT) and the PTP Master
  - DUT probe produces PDV result data in Symmetricom Timemonitor format
  - DUT in slave mode output 1PPS and allows measurement of 1PPS performance.



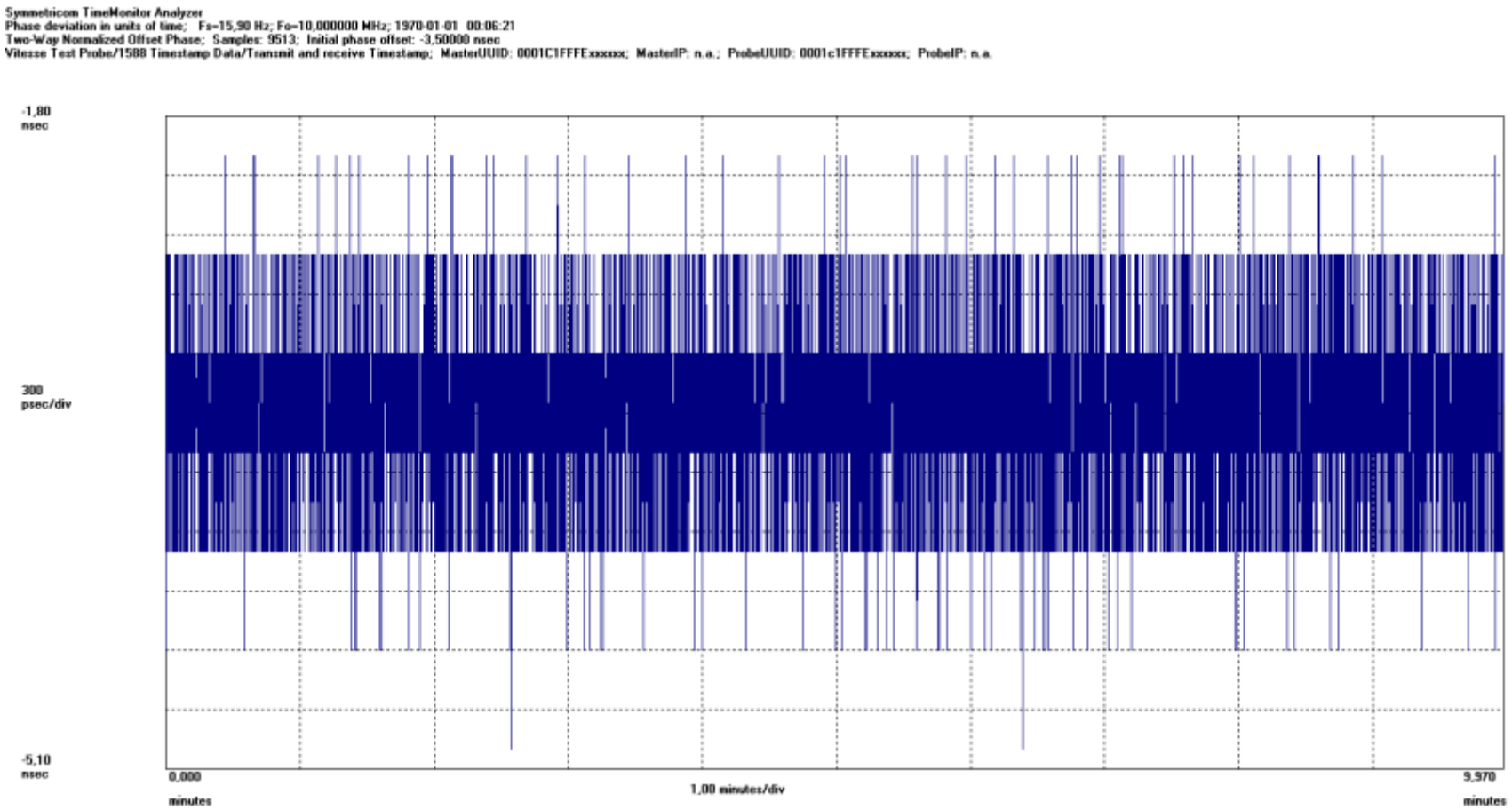
VSC8490 Test Result

- **Easily meets the Class B limit**
  - See details in the following slides

VSC8490	Test result w/o MACsec	Test result with MACsec	Class B limit
Constant Time Error, cTE	-3.3 ns	2.9 ns	20 ns
Dynamic Time Error MTIE (filtered)	157 ps	420 ps	40 ns
Dynamic Time Error MTIE (unfiltered)	4 ns	4 ns	
Dynamic Time Error TDEV (filtered)	14 ps	35 ps	4 ns
Dynamic Time Error TDEV (unfiltered)	460 ps	400 ps	
Maximum Time Error (unfiltered)	5.0ns	4.5 ns	70 ns

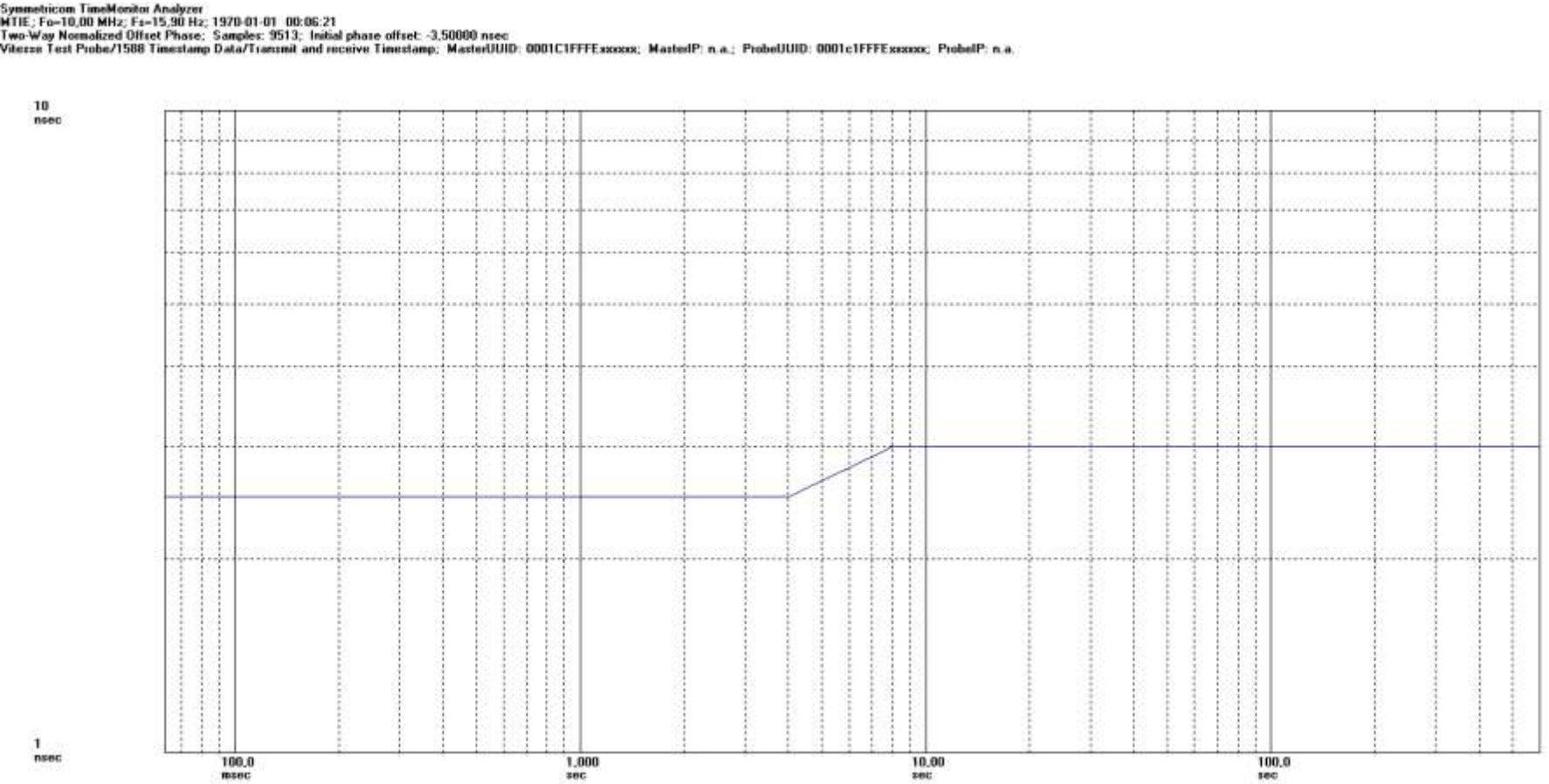
VSC8490 TE(t) - Unfiltered

- LAN mode without MACsec enabled



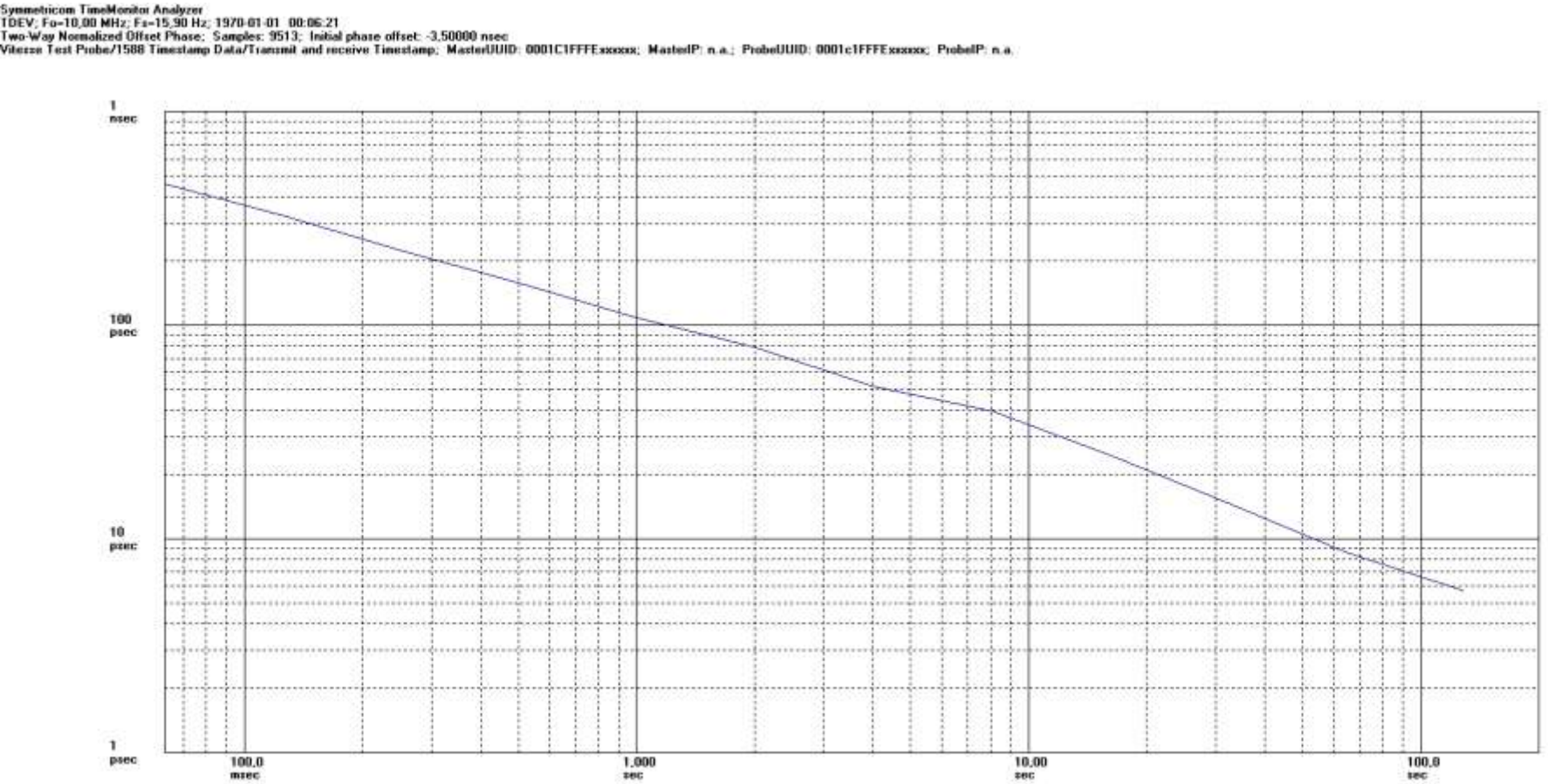
VSC8490 dTE MTIE - Unfiltered

- LAN mode without MACsec enabled – 4 ns



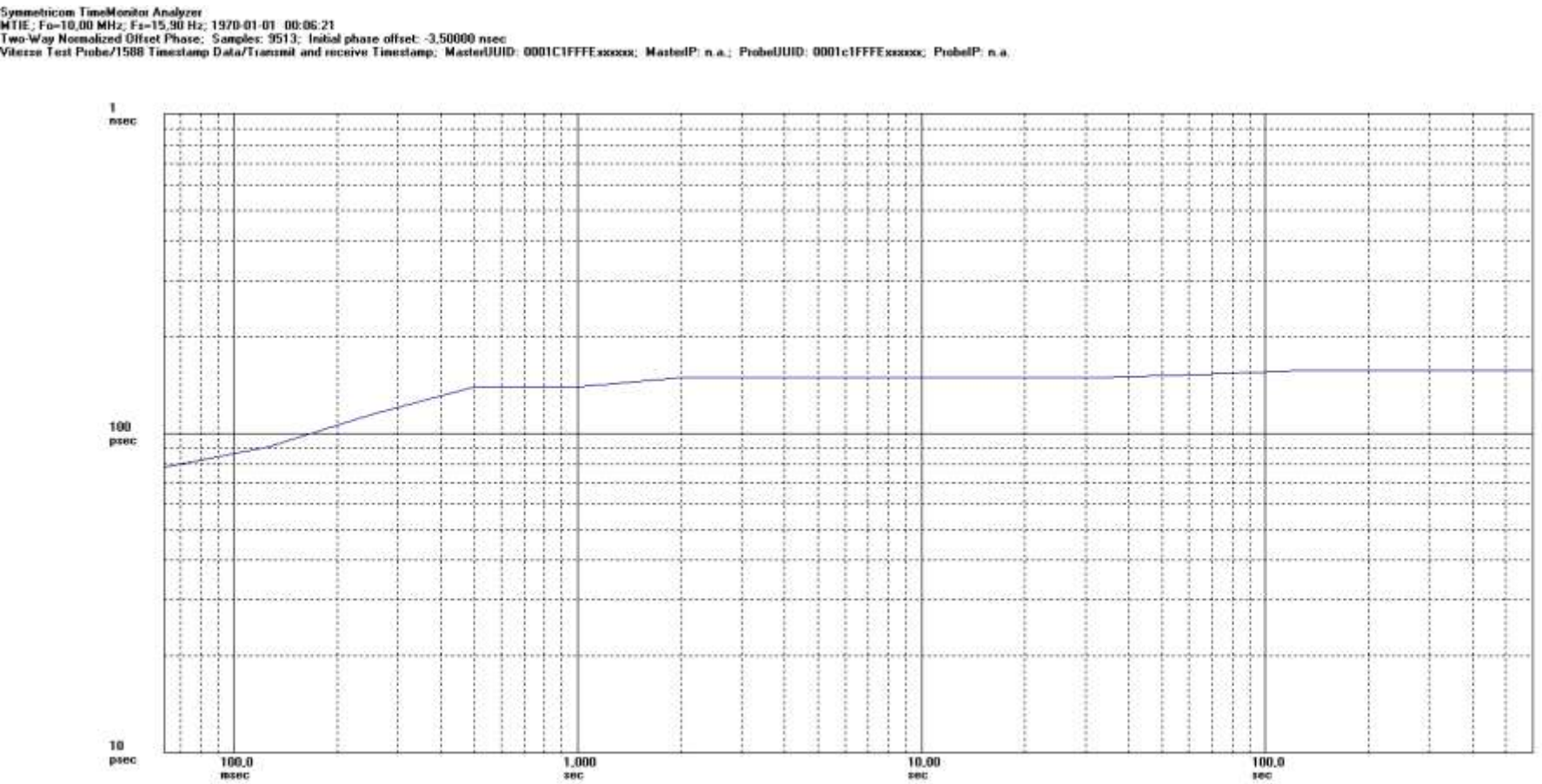
VSC8490 dTE TDEV - Unfiltered

- LAN mode without MACsec enabled – 460 ps



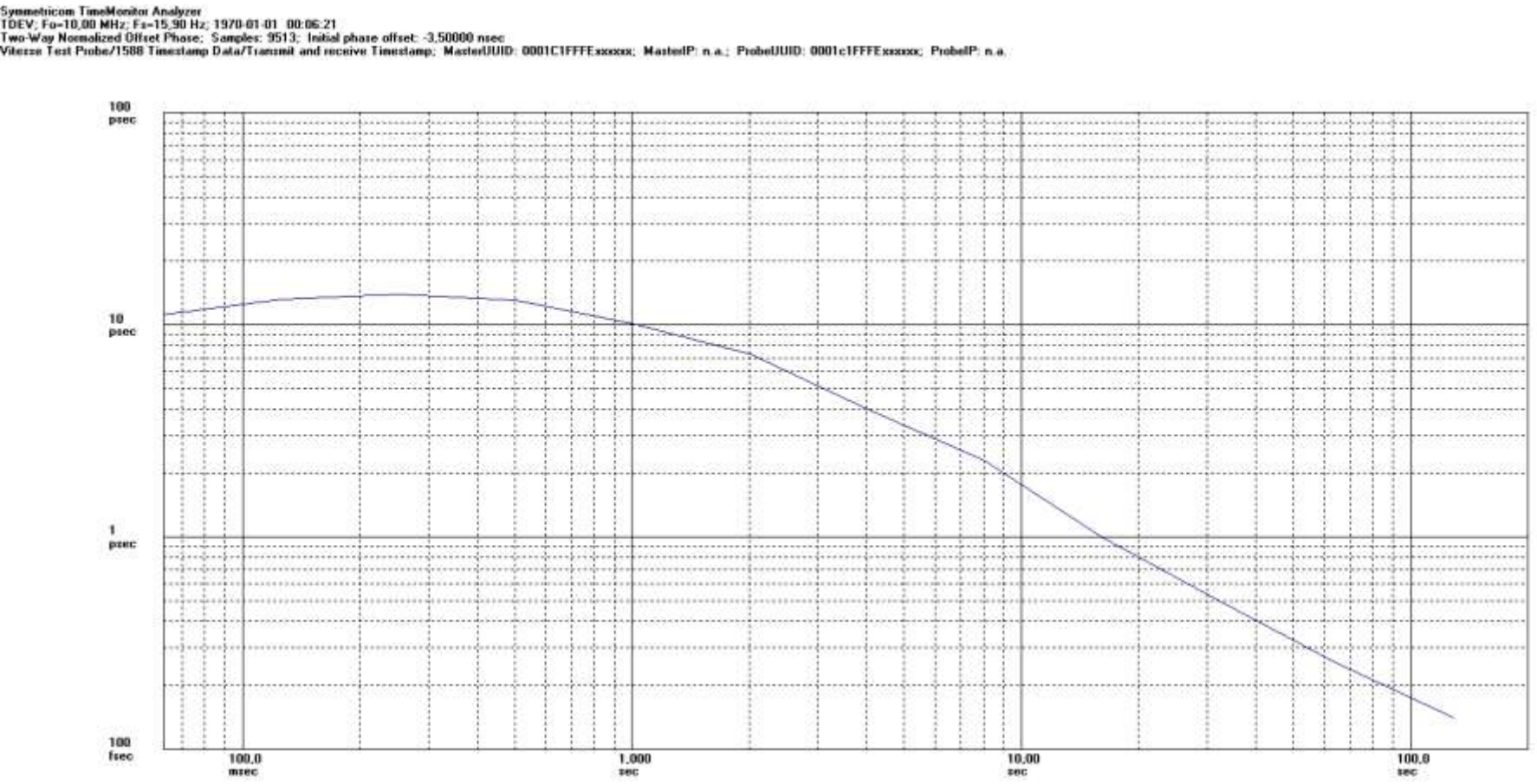
VSC8490 dTE MTIE - Filtered

- LAN mode without MACsec enabled – 157 ps



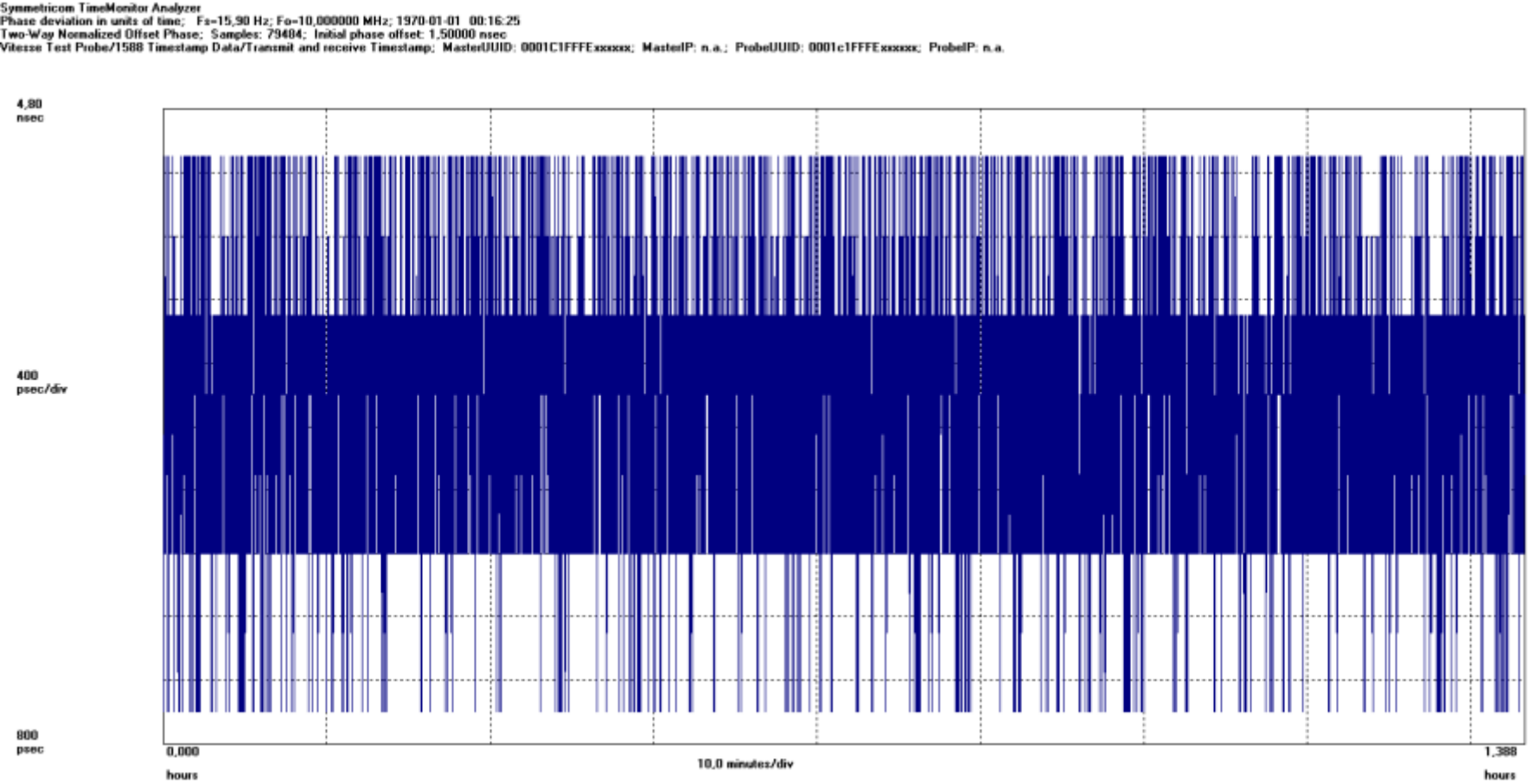
VSC8490 dTE TDEV - Filtered

- LAN mode without MACsec enabled – 14 ps



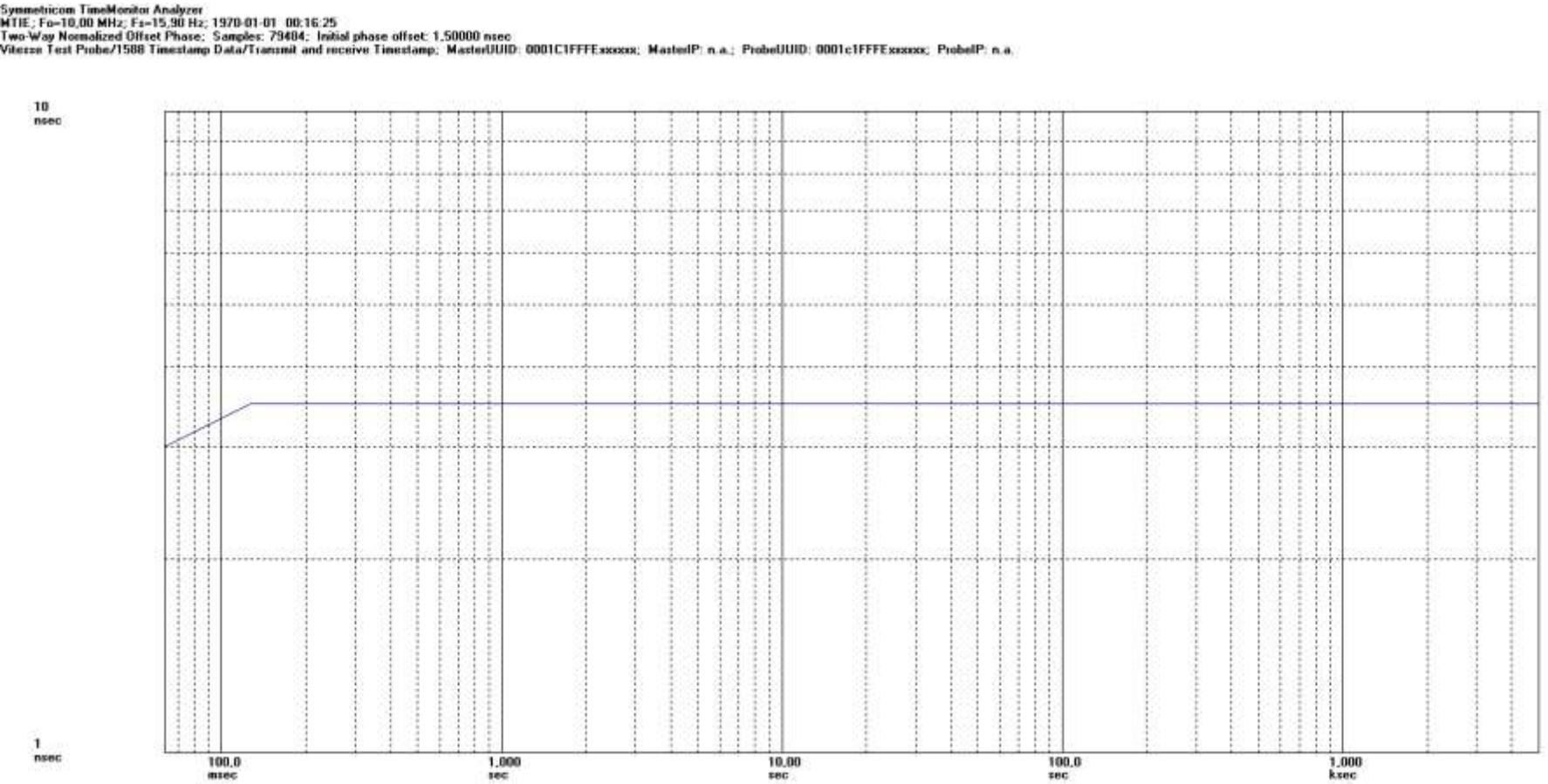
VSC8490 TE(t) - Unfiltered

- LAN mode with MACsec enabled



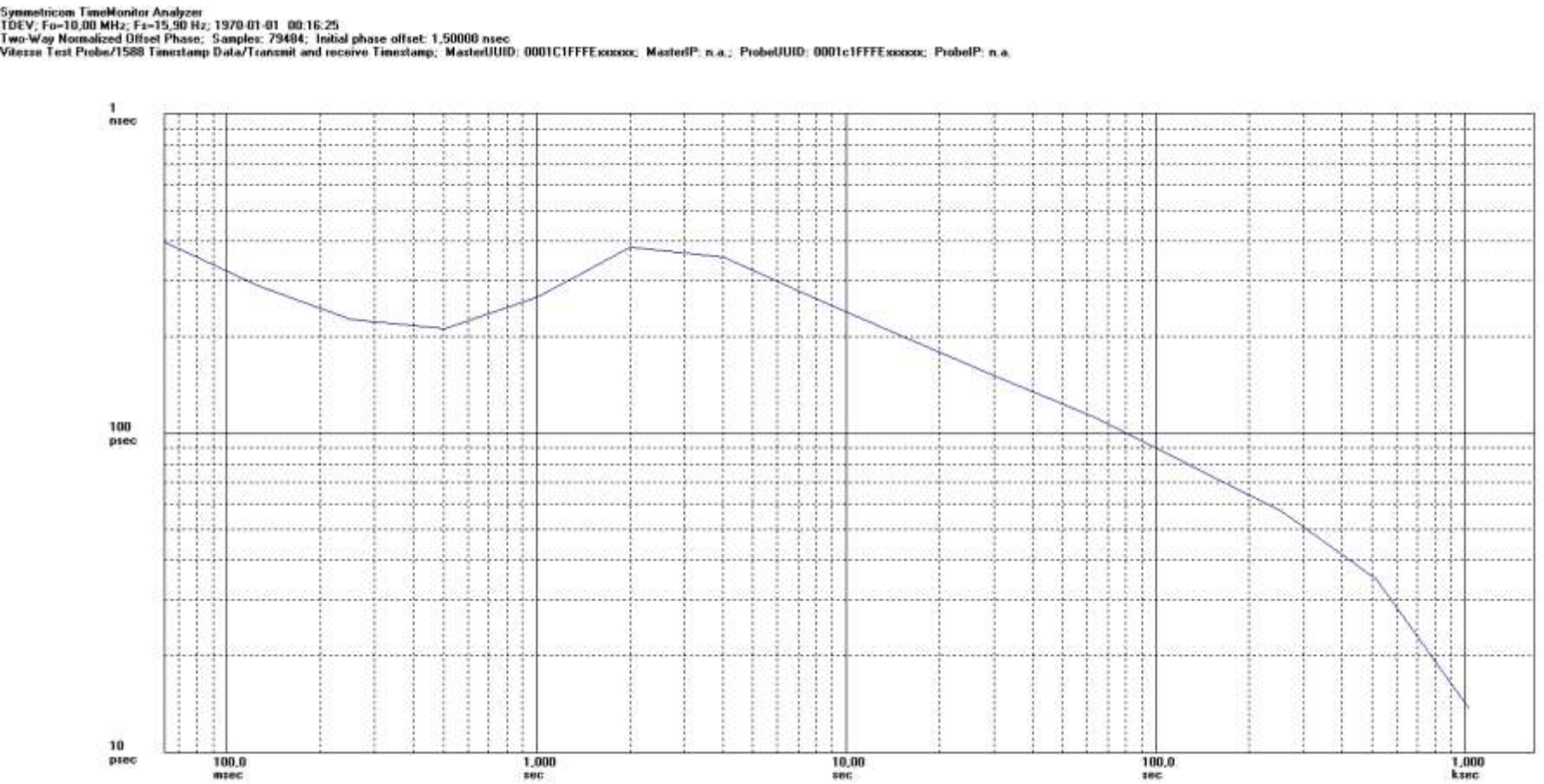
VSC8490 dTE MTIE - Unfiltered

- LAN mode with MACsec enabled – 4 ns



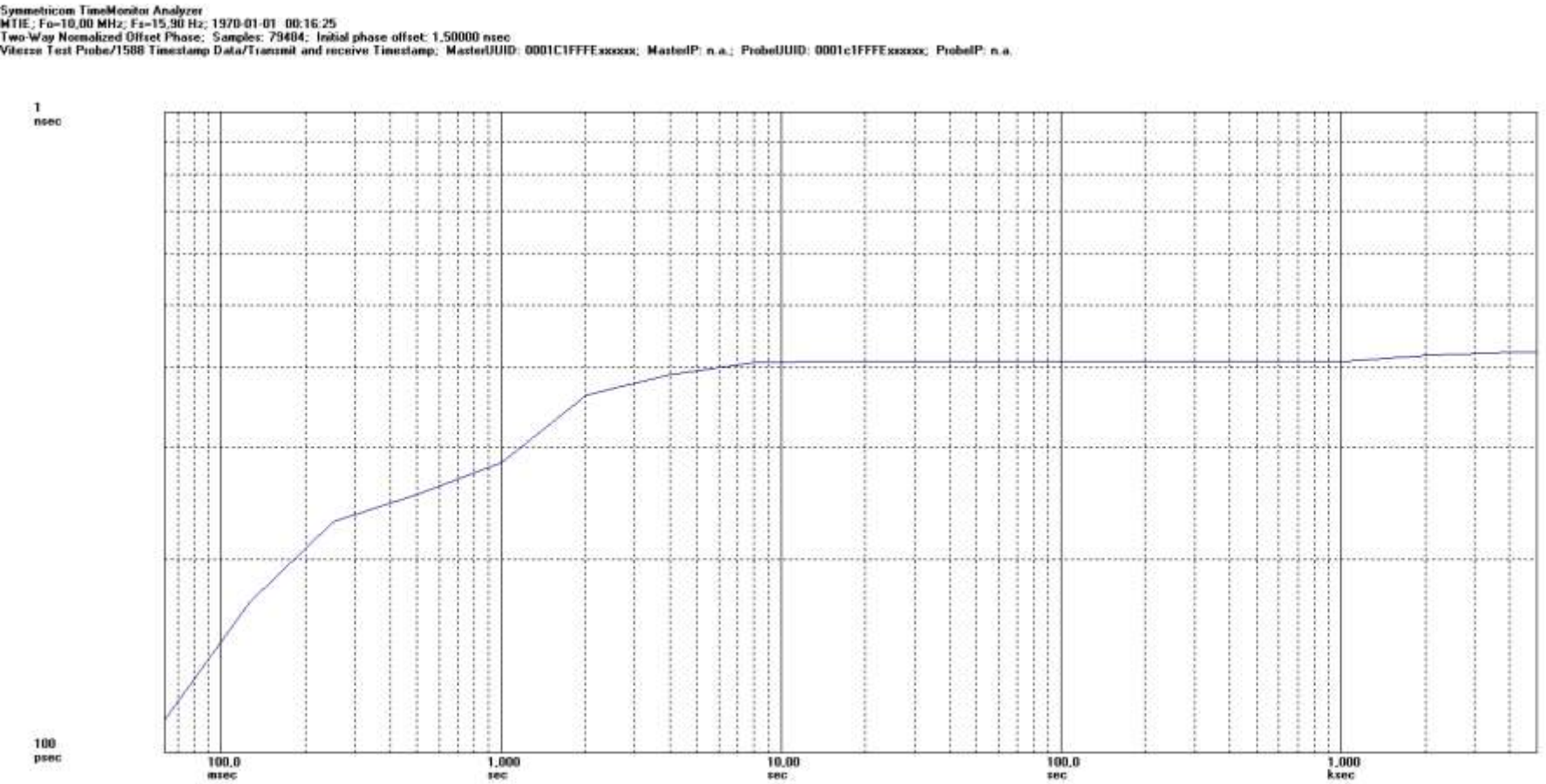
VSC8490 dTE TDEV - Unfiltered

- LAN mode with MACsec enabled – 400 ps



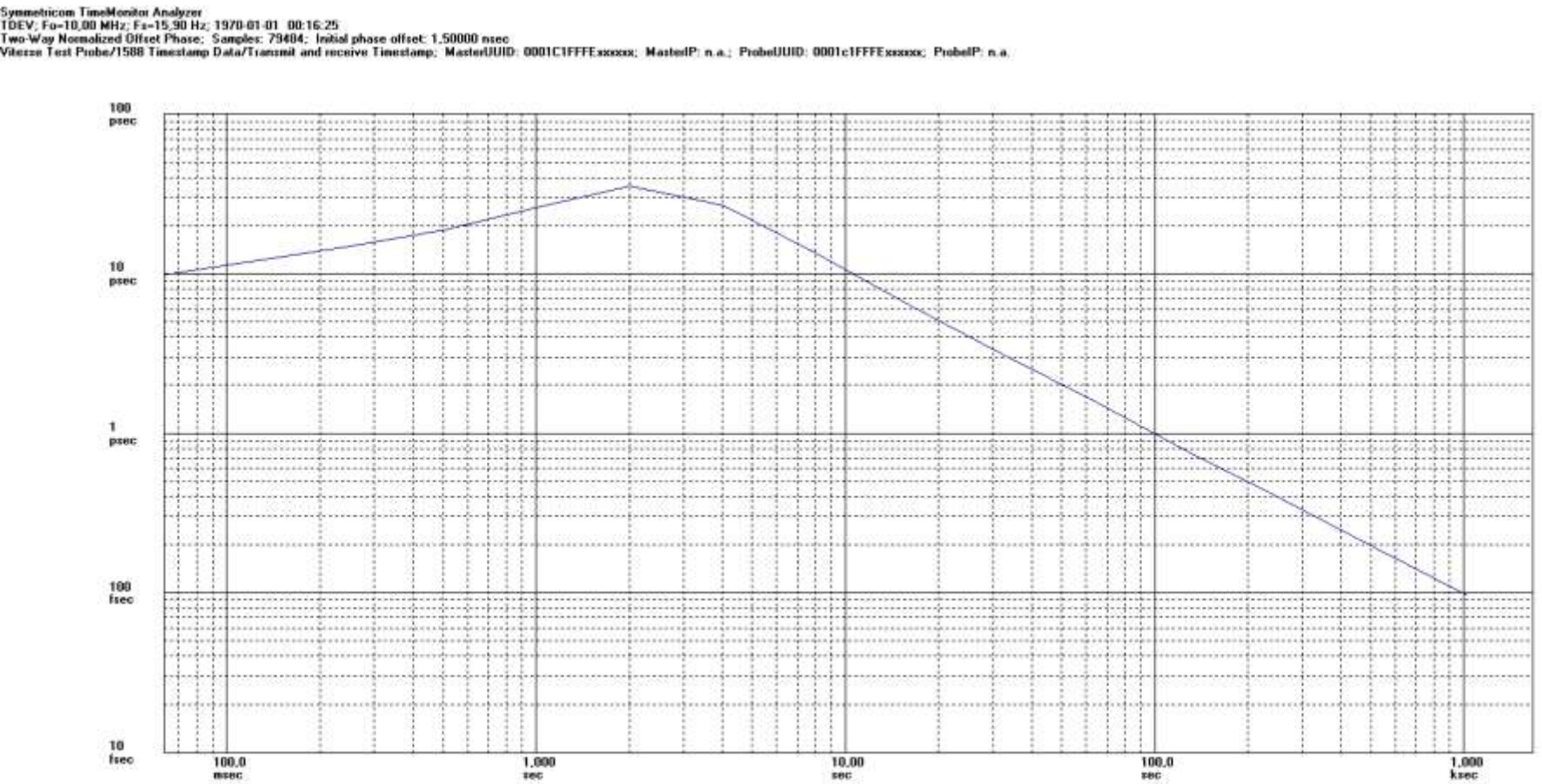
VSC8490 dTE MTIE - Filtered

- LAN mode with MACsec enabled – 420 ps



VSC8490 dTE TDEV - Filtered

- LAN mode with MACsec enabled – 35 ps



Summary And Conclusions

- PTP is now being used to provide timing and synchronization with insufficient physical security
- Protecting the PTP traffic by means of encryption and/or integrity protection is needed.
- IPsec is often used for data traffic, but this is not a practical solution for accurate PTP transfer that needs hob-by-hop support.
- IPsec is not a good security solution for PTP due to the large and variable processing delays.
- MACsec is a layer 2 encryption protocol that is a perfect fit for protection of PTP traffic – hob-by-hob, or end-to-end.
- It is shown how MACsec can be used to protect the PTP traffic without impacting the accuracy and how MACsec can be easily implemented in a systems architecture.

Thank You

VITESSE®

Making next-generation networks a reality.