Timing over MACsec

Secure 1588: Another Step Towards True Cloud Service Delivery

Highly accurate coordination of time is an essential part of operating many distributed systems including power grids, water and gas distribution systems and mobile communications networks, as well as in industrial automation. Precision Time Protocol (PTP), defined in IEEE 1588, is used in all of these applications for time distribution.

Continued Internet traffic growth, combined with the trends towards SDN and virtualization, will compel businesses, utilities and manufacturers to deliver on-demand access to resources and on-time delivery services. Thanks to the Internet of Things (IoT) and machine-to-machine (M2M) communications, all three can leverage the same cloud networks to compete and provide more differentiated services.

With today's connected world greatly dependent on reliable access to services – such as electricity and water, Internet and mobile services, and efficient manufacturing of goods – virtually any sector is vulnerable to cyber threats, making security solutions to protect operations a must. Here is when a particular data security solution comes to play: MACsec data encryption, as defined in the IEEE 802.1AE standards and as implemented by Microsemi, can be used to eliminate threats on vulnerable Ethernet links – within substation and factory environments, over metro wide cloud connections and even connections over third-party Ethernet service providers – all while maintaining timing accuracy.

The need for a combined solution is clear: MACsec must secure the PTP distribution tree.

For tight network synchronization, PTP requires accurate timestamping of the packet. However, MACsec requires insertion and removal of the 24-to-32-byte long MACsec header on all or some of the frames on the link, causing large delay variations between the egress timestamping point and the link connector (and similarly on the ingress). The PTP protocol assumes that the delay on a link is constant. With MACsec, however, this is not the case.

Encryption and timing accuracy have historically been incompatible. Microsemi has solved this challenge with its Intellisec™ PHYs, which fully preserve timestamping accuracy on a MACsec-enabled link.

Figure 1 shows an example of using PTP over MACsec technology in a power sub-station application. The LAN connections inside the stations are MACsec-secured, as are the WAN ports connecting the stations. At each station, a GNSS-signal feeds the Grand Master, which distributes time to all units that require so using IEEE 1588/PTP. It is further illustrated how the Grand Master at Sub-Station n offers a back-up timing reference for the Grand Master in Sub-Station n+1, should the GNSS-reference there fail for some reason.

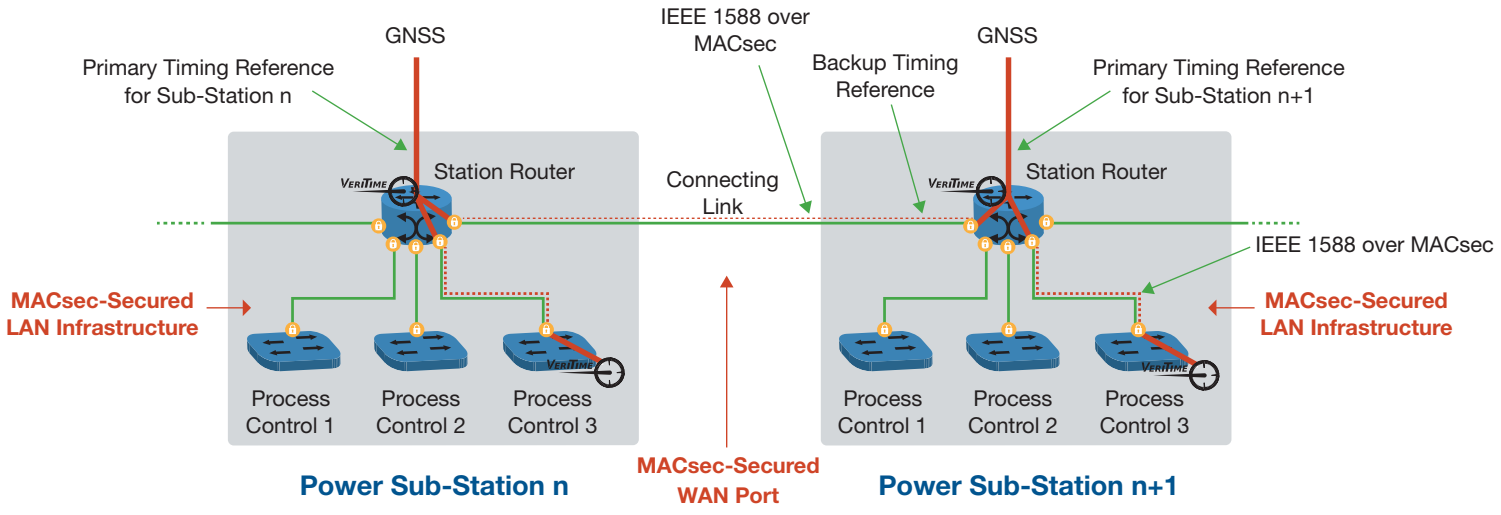

Figure 1. Using PTP over MACsec in a power sub-station application

Timing over MACsec

Using Microsemi Intellisec™ and VeriTime™ PHYs, the dynamic MTIE performance shown below is possible (Slave connected with Master over a single MACsec-secured Ethernet link at 10 Gbps).

Microsemi VSC8490 PTP-enabled PHY	Test result Without MACsec	Test result With MACsec	ITU G.8273.2 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)	5.0 ns	4.5 ns	70 ns

Figure 2. Dynamic MTIE Performance with Microsemi Secure 1588 Solution

Secure 1588 PHY Solution Highlights

- Enables "Bump-in-the-Wire PHY" which incrementally adds MACsec via simple software upgrade
  - 128-bit MACsec (802.1AE-2006) and 256-bit MACsec (802.1AEbn-2011)
  - Extended Packet Numbering (XPN, 802.1AEbw-2013)
- Enables Timestamping for IEEE 1588 and Ethernet/MPLS OAM packets
  - Timestamping and MACsec supported simultaneously with **no loss of 1588 accuracy**
  - 1588/OAM delivery over advanced encapsulations such as Q-Q, IP/MPLS, Pseudo wire
- Enables (patent-pending) VLAN tag and MPLS label bypass features
  - Provides advanced end-to-end encryption services over Carrier Ethernet
  - Interoperable with standard-compliant implementations
  - Select network control packets may be left unencrypted for network use
  - PTP, OAM, etc.
- Available in multiple physical transceiver solutions by Microsemi
  - VSC8584: 100/1000BASE-T operation
  - VSC8490/VSC8258: 10 Gbps LAN operation

Cloud-based data collection and service delivery are major catalysts of both the emerging smart grid and Industry 4.0 paradigms, where users need to collaborate and collect real-time data securely and reliably. Secure 1588 solutions, combining security and uncompromised timing over Ethernet, will be essential to enabling true cloud service delivery. Microsemi is leading the way with such a solution: using Intellisec MACsec authentication and data encryption technology to secure the PTP distribution tree.

Secure 1588 is a reality. To learn more, visit www.microsemi.com/products/physical-layer.

Microsemi Corporate Headquarters
One Enterprise, Aliso Viejo, CA 92656 USA
Within the USA: +1 (800) 713-4113
Outside the USA: +1 (949) 380-6100
Sales: +1 (949) 380-6136
Fax: +1 (949) 215-4996
email: sales.support@microsemi.com
www.microsemi.com

Microsemi Corporation (Nasdaq: MSCC) offers a comprehensive portfolio of semiconductor and system solutions for communications, defense & security, aerospace and industrial markets. Products include high-performance and radiation-hardened analog mixed-signal integrated circuits, FPGAs, SoCs and ASICs; power management products; timing and synchronization devices and precise time solutions, setting the world's standard for time; voice processing devices; RF solutions; discrete components; security technologies and scalable anti-tamper products; Ethernet solutions; Power-over-Ethernet ICs and midspans; as well as custom design capabilities and services. Microsemi is headquartered in Aliso Viejo, Calif., and has approximately 3,600 employees globally. Learn more at www.microsemi.com.