Navigating Advanced Features of PTP to Enable Higher Timing Accuracy and Security in Complex Networks

A Leading Provider of Smart, Connected and Secure Embedded Control Solutions

Samer Darras
Barry Dropping

Agenda

- Why is improving accuracy and security for PTP important
- What tools are the latest PTP standards releases enabling
- Accuracy enhancements and implementations
- Security enhancements and implementations
- Conclusions and future direction

Why is Improving Accuracy and Security for PTP Important

- **Our collective mission is to <u>generate</u>, <u>distribute</u>, and <u>apply</u> timing and synchronization**
- **IEEE® 1588 PTP is primarily a <u>distribution</u> technology**
- **Critical application questions:**
  1. Is it accurate enough
  2. Is it secure enough

IEEE® 1588 PTP Standards

- **IEEE® 1588-2019 Precision Time Protocol (PTP)**
  - IEEE 1588a-2023 Amendment introduces a new TLV to enable increased timing accuracy in complex networks
  - IEEE 1588 four-prong security model for PTP network deployments

MICROCHIP

IEEE 1588a-2023 Amendment Highlights

- **TLV Extension for Enhanced Accuracy Metrics**
  - Improved path selection for BMCA
- **Error models for quantifying path error components**
  - Quantifies total path error for TLV Extension

Why Is the Enhanced Accuracy TLV Needed?

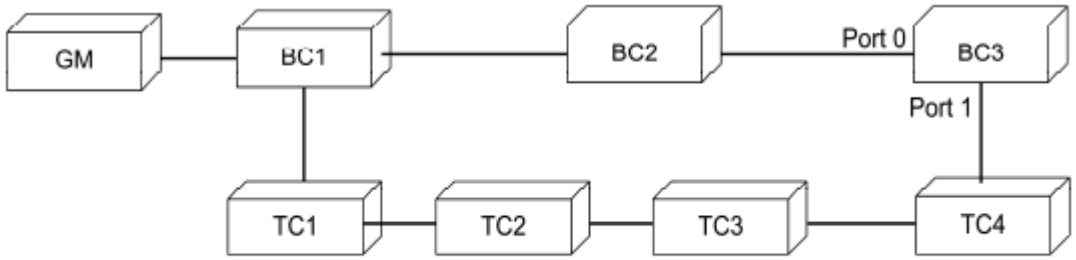


Figure P2.1—Behavior of the default BMCA in a network with a chain of TCs

- **Issue 1: The default BMCA does not count TCs as a hop**
  - BC3 sets port 1 as slave even though the path goes through a larger number of element hops (TCs)

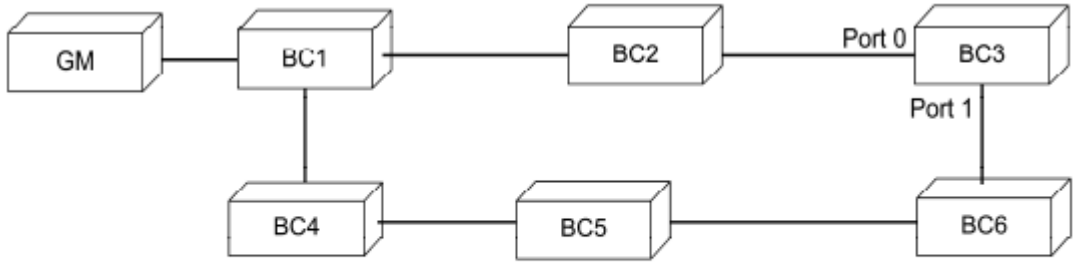


Figure P2.2—Behavior of the default BMCA in a network with chains of BCs providing different synchronization performance.

Source IEEE Std 1588a-2023

- **Issue 2: The default BMCA picks the lowest hop count, but not all BCs are equal**
  - BC4/BC5/BC6 path has lower total error than the BC2 path, but BC3 sets port 0 as slave due to lower hop count

BMCA – Best Master Clock Algorithm
TC – Transparent Clock
BC – Boundary Clock

MICROCHIP

Enhanced Accuracy TLV Error Components

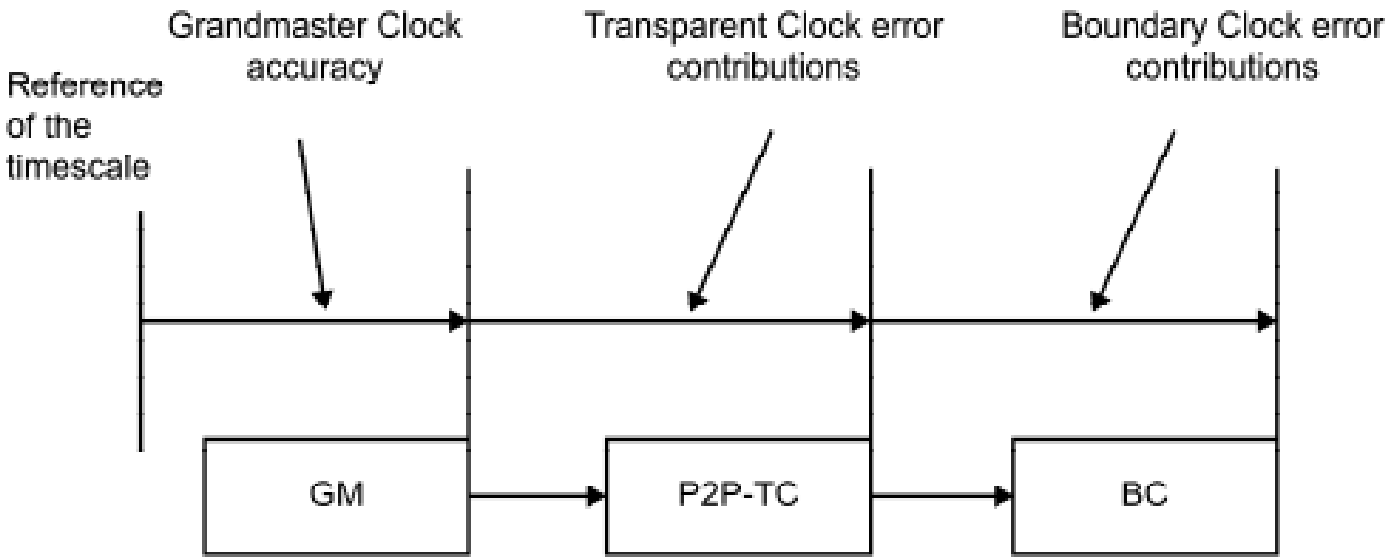


Figure 46—Contribution of the various PTP Instances to metrics in the TLV

Source IEEE Std 1588a-2023

- **The TLV includes two groups of components**
  - GM component
  - Distribution components
- **Error components are categorized as transient or steady state (dynamic and static)**

Enhanced Accuracy TLV Format

- **Enhanced Accuracy TLV is included in the GM announce message**
  - Adds TC hop count and various transient, dynamic, and static error estimate fields
  - TLV aware distribution elements update as the TLV message is propagated forward

Table 130 —ENHANCED_ACCURACY_METRICS TLV format

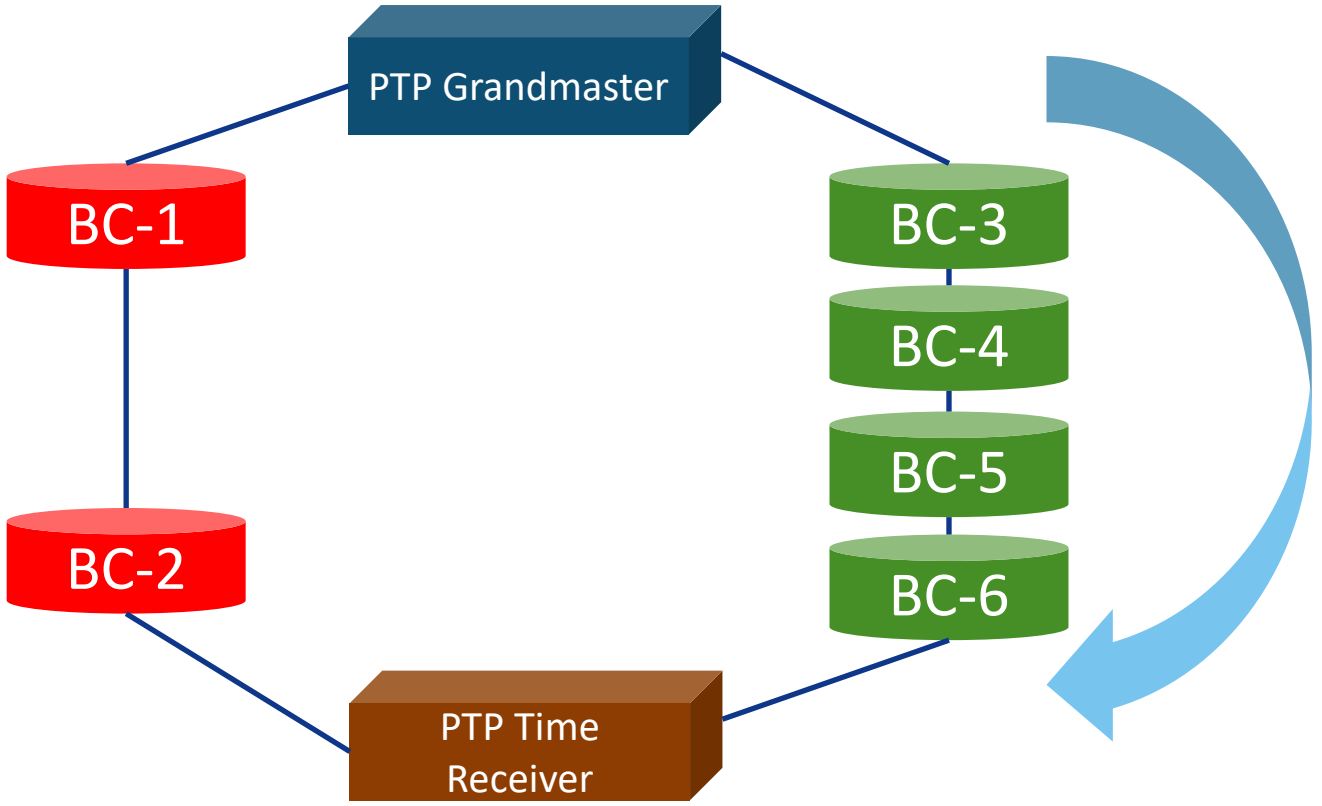
Bits								Octets	TLV offset
7	6	5	4	3	2	1	0		
tlvType								2	0
lengthField								2	2
bcHopCount								1	4
tcHopCount								1	5
exclusionFlags ~~Reserved~~								2	6
maxGmInaccuracy								8	8
varGmInaccuracy								8	16 [a]
maxTransientInaccuracy								8	24 [a]
varTransientInaccuracy								8	32 [a]
maxDynamicInaccuracy								8	40 [a]
varDynamicInaccuracy								8	48 [a]
maxStaticInstanceInaccuracy								8	56 [a]
varStaticInstanceInaccuracy								8	64 [a]
maxStaticMediumInaccuracy								8	72 [a]
varStaticMediumInaccuracy								8	80 [a]

Source IEEE Std 1588a-2023

MICROCHIP

Key Benefit of the Enhance Accuracy TLV

Low precision class A BCs provide the less accurate path (100ns per hop)



High precision class D BCs provide the most accurate path (5ns per hop)

Enables the BMCA to select the most accurate path rather than the path with the fewest hops.

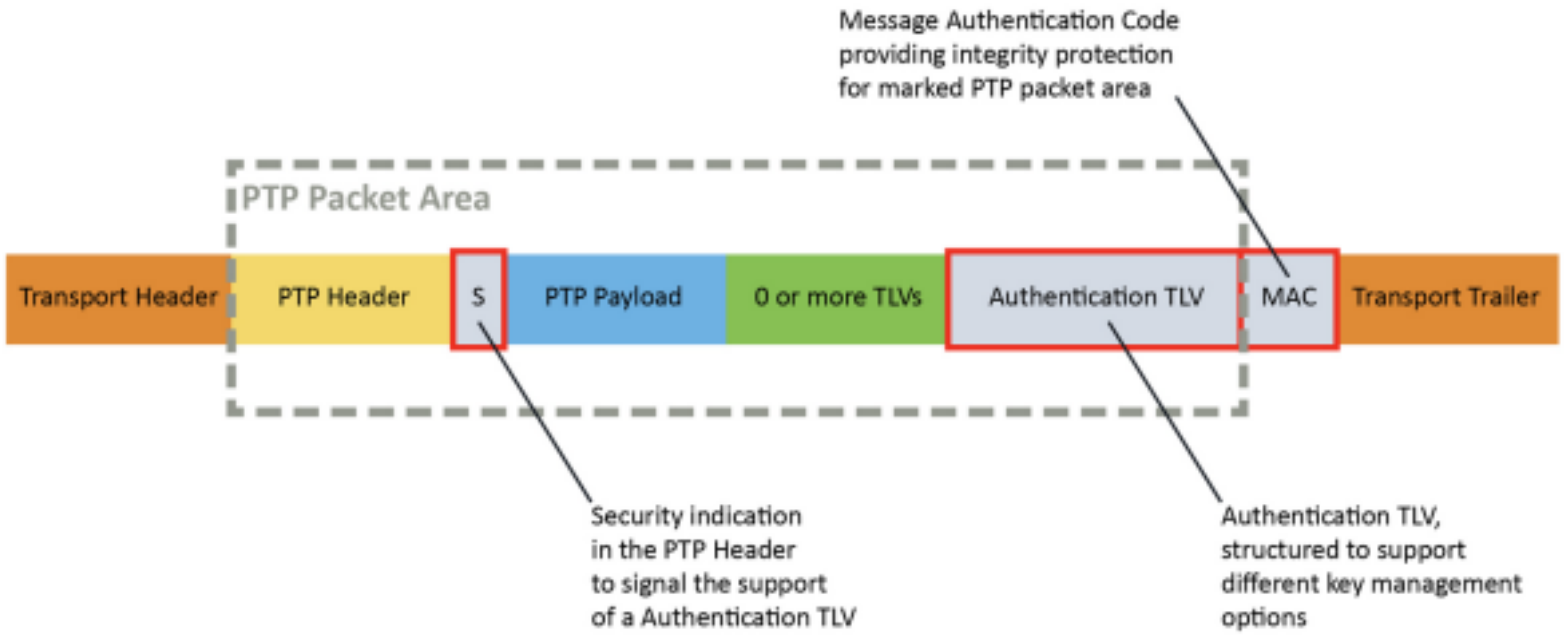
MICROCHIP

Four Prong Security Model

PTP Security Enhancements

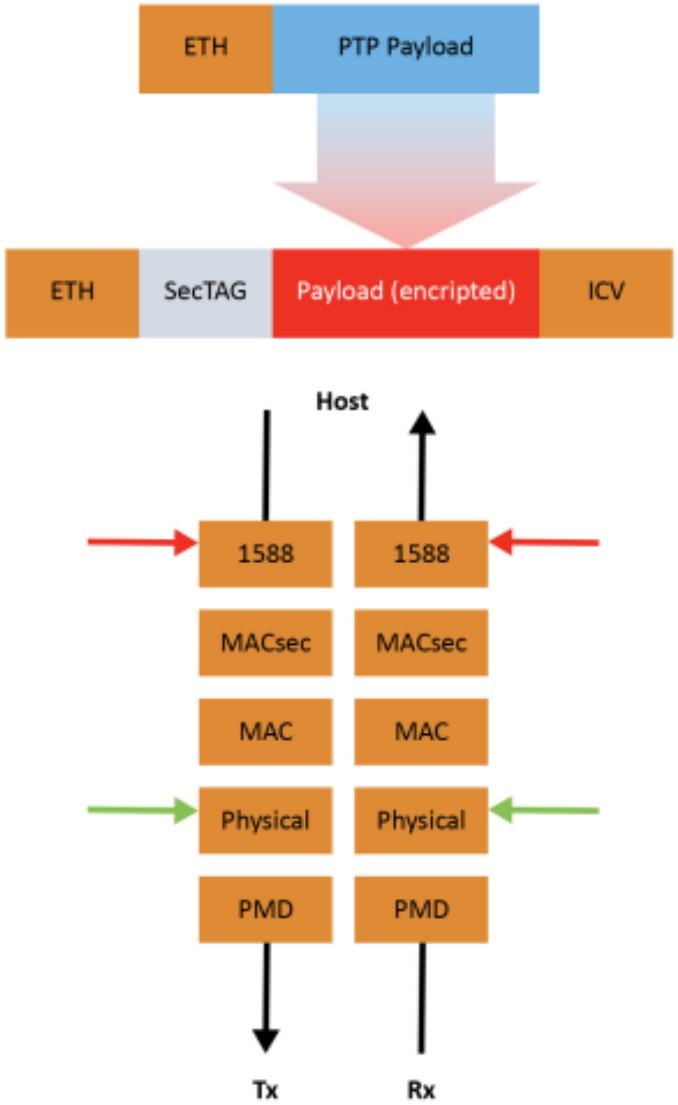
- IEEE® 1588 2019 introduces a four-prong security model
  - Prong A – Integrated Security Mechanism
  - Prong B – External Security Mechanisms
  - Prong C – Architecture Guidance
  - Prong D – Monitoring and Management

Prong A – Integrated Security Mechanism



- **Key challenge to implement Prong A is that security key distribution for the Authentication TLV has not been finalized**
- **There are proposals to use Network Time Security Key Exchange (NTS-KE) for both NTP and PTP**

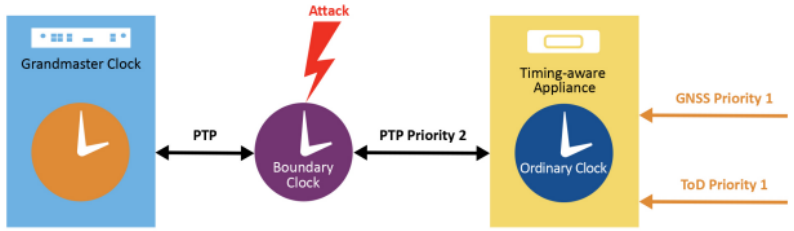
Prong B – External Security Mechanisms



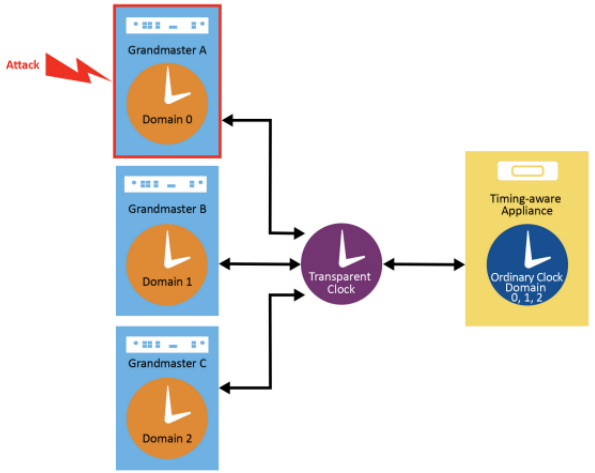
Encompasses using well known transport security mechanisms such as MACsec (Media Access Control Security) and IPsec (IP Security) for securing PTP

- MACsec implementations lagging because they require HW upgrades.
- IPsec accuracy concerns remain as a barrier

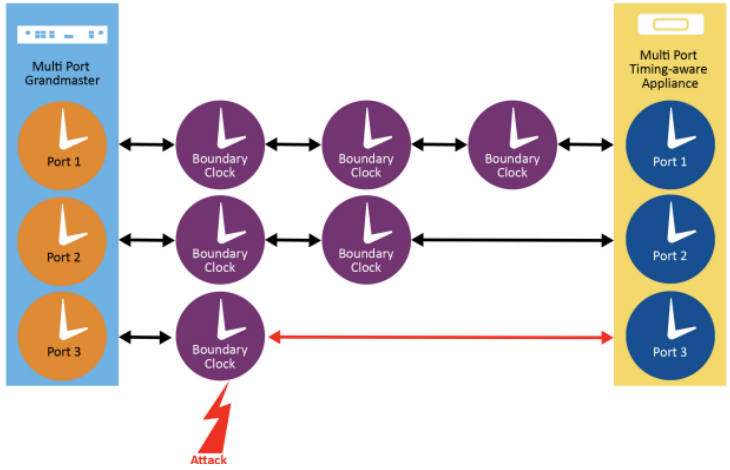
Prong C – Architecture Guidance: Widely Deployed Today



Multiple Inputs using various timing systems



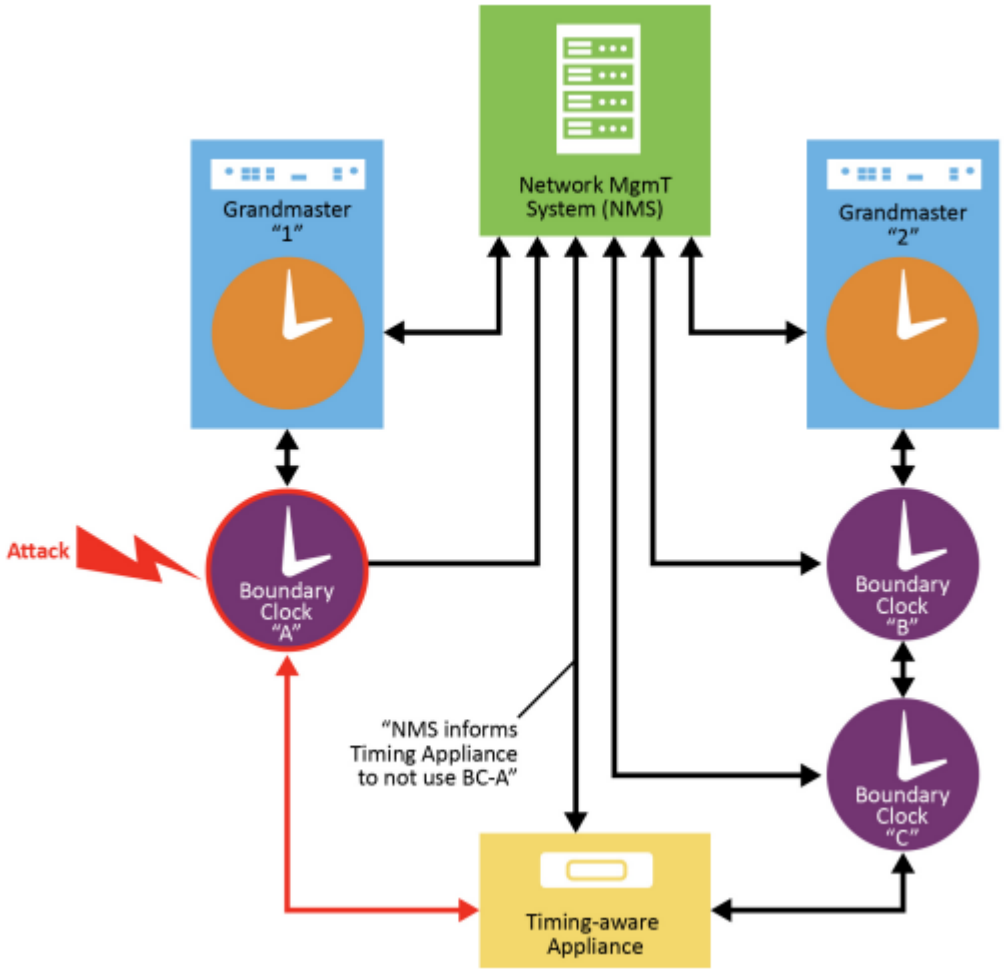
Multiple PTP Grandmasters with Different Domains



Timing Appliance Using Multiple Paths

MICROCHIP

Prong D – Monitoring and Management



Monitoring and management provides a higher view of the network topology and can monitor all devices and network changes. Upon detection of an attack on grandmaster or path, it can inform a timing appliance to stop using the grandmaster or path for time synchronization

MICROCHIP

Conclusions and Future Direction

- **PTP accuracy**
  - Enhanced Accuracy TLV as defined in IEEE 1588a-2023 Amendment support in various industry PTP profiles to drive adoption and deployment
- **PTP Security**
  - Start with Prong C and D for security today – widely deployed
  - Prong A and B will come as future standards activities progress

Thank You