P802.DP Time Sync

Availability and Integrity for Aerospace

Abdul Jabbar
GE Research

Objective

- **Review integrity and availability requirements for aerospace**
- **Review 802.1AS features to support aerospace requirements**
- **Identify features, options, configurations, procedures for AS based time sync for aerospace**
- **Identify changes, if any, required in base standards**

Aerospace Base Requirements

Characteristics

- Fully engineered – end stations, bridges, and links are fully characterized before runtime
- Static networks – no changes post design and qualification
- Centrally managed and configured – in one TSN domain
- Requires both high availability and high integrity
- Requires certification for most use cases. Impact on repeatability, dormant code, (code) complexity, etc.

Prior discussed PTP requirements

- External Port Configuration; No BMCA; No higher-level (re)configuration during operation
- Arbitrary timescale

Proposal: Amend 802.1AS to remove the mandatory requirement for a PTP instance to support domain 0…and therefore BMCA and PTP Timescale. The domain 0 behavior remains unchanged.

How: Amend 802.1AS via P802.1ASdm. Comment on next TG ballot.

Time Synchronization Requirements for Aerospace

Performance:

- 90% use case coverage: 1 usec accuracy across 5 hops (max time error relative to GM = +/- 500 nsec)
- 99% use case coverage: 1 usec accuracy across 15 hops (max time error relative to GM = +/- 500 nsec)
- There will always be a tail…can never say anything about 100% coverage. Previously discussed that the AS does not exclude better performance implmentations.

Availability:

- High availability in the presence of link, bridge, end station, and GM faults and failures
    - Requirement to tolerate multiple (typically 2) simultaneous arbitrary faults
- System design is responsible for achieving the desired level of availability utilizing PTP and non-PTP solutions
- PTP can enable/support that design with native redundancy features (e.g., Hot standby, multiple domains and instances)

Time Synchronization Requirements for Aerspace

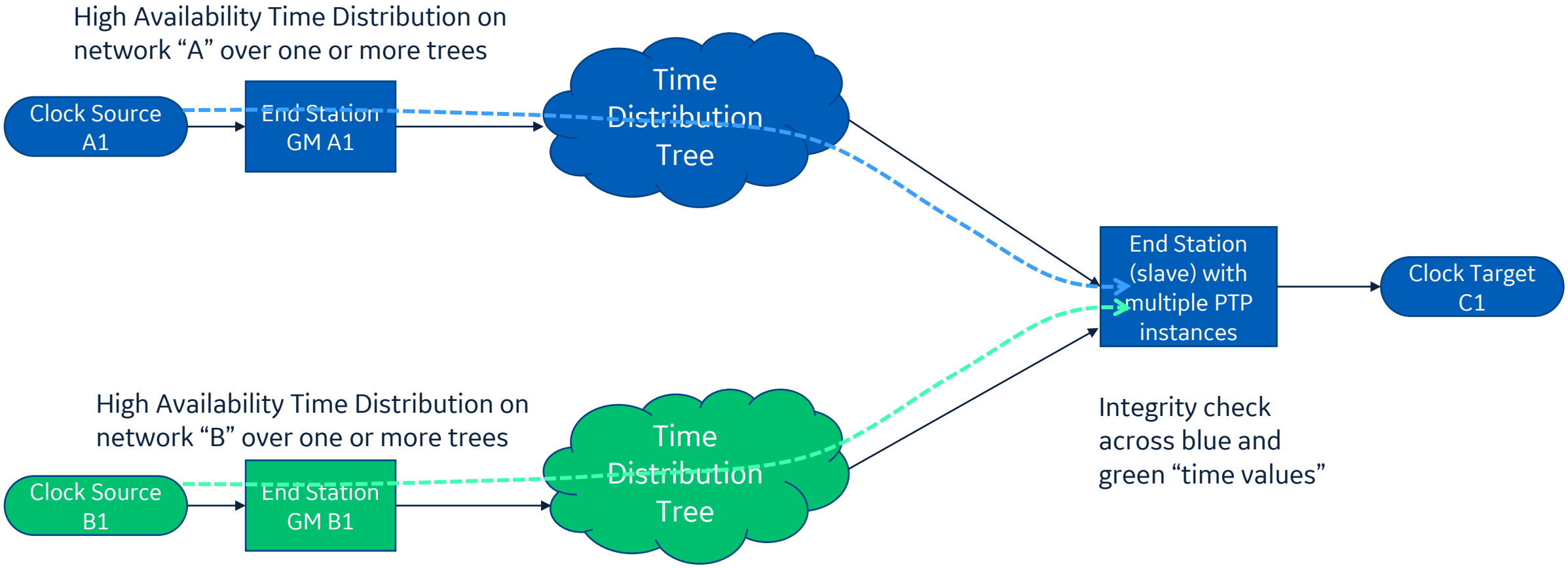
Integrity:

- High time integrity in the presence of link, bridge, end station, and GM faults and failures
    - Requirement to tolerate multiple (typically 2) simultaneous arbitrary faults
- Since PTP requires computations along the network path, end-to-end (higher-level) integrity mechanisms do not work. PTP must natively address integrity.
- System design is responsible for achieving the desired integrity level utilizing mostly/exclusively PTP features
- Under faulty conditions, a correctly operating end station shall be able to maintain the target max time error relative the correctly operating GM. If unable to maintain the max time error, the correctly operating end station shall detect an erroneous time sync state.
    - Assumes that system design provides for a non-faulty time distribution tree between the clock source and clock target

802.1AS Components to support Aerospace Requirements (Working Slide)

1. Multiple GMs
    1. Externally synchronized (outside of PTP)
    2. Synchronized via PTP
2. Multiple domains in the network
    1. Separate domains
    2. Time transfer within domains (e.g. ASdm split functionality)
3. Multiple PTP instances at end stations (typically 3, but different number are allowed)
4. Method to drive clock target using multiple PTP instances
    1. Outside of PTP
    2. Inside PTP (do it as part of the profile)
5. Redundant paths of for a given domain

Trivial (Abstract) Example



More than two “colors” possible…

Trivial Example – Potential use of Hot Standby