Time Sync – Redundant Grandmaster Clock Support.

IEEE 802.1
May 2013 Interim

Presented by

Eric Spada & Yong Kim

Rationale and Methods

- Rationale – Seamless transition (frequency and phase) from primary Grand Master (pGM) to backup Grand Master (bGM) under failure conditions.
  - Backup GM is provisioned as active (sending sync) or passive (not sending sync).
  - Switching between GMs (pri -> backup and backup->pri) must be seamless (controlled phase and frequency deviation).
- Methods – Need to support redundant grand master clocks, that are synchronized to each other.
  - Feature definition needed in Stds.
  - Proposal in following slides.

- Prior presentations on its needs and related topics:
  - www.ieee802.org/1/files/public/docs2011/as-kweber-syncRedundancy-110914.pdf
  - http://www.ieee802.org/1/files/public/docs2012/new-avb-wsteiner-failure-modes-for-8021ASbt-1112-v01.pdf
  - http://www.ieee802.org/1/files/public/docs2012/new-avb-wsteiner-fault-hypothesis-and-redundancy-management-0912-v01.pdf

Simultaneous Redundant GM

- Operating.
  - Case 1: pGM and bGM have the same primary clock source (e.g. GPS) and are thus synchronized
  - Case 2: bGM is syntonize to the pGM by processing the Sync messages as a boundary clock.
    - bGM syntonized clock should be as stable as needed per use case MTIE.
  - Failure detect by bGM is the same in both cases, it stops received Sync from the pGM i.e. as Sync timeout occurs.
  - Devices (Ethernet Stations) receive pSync & bSync from both the pGM and bGM at nominally twice the rate as with a single GM. These messages look identical from a synchronization perspective (Clock ID are different for management purposes)
- pGM Failure Operation using Active bGM:
  - bGM continues to send Sync to all devices in network.
  - Devices receive pSync & bSync from both the pGM and bGM at twice the rate as with a single GM.
  - These Sync messages look identical from a synchronization perspective (Clock ID are different for management purposes)
  - Devices process these messages as if they were the same GM since they are synchronized.
- pGM Failure Operation using Passive bGM:
  - bGM starts sending Sync messages after timeout of pGM.
  - Device are in hold-over until bGM synchronization is achieved with bGM.
    - Clock source is consider the same: BMCA GM selection algorithm unmodified/configured and does not act.
      - Dual time-domain could be extended to cover overlapping pSync and bSync timing path.
    - Clock source is considered different: BMCA GM selection may need to be configured.

Simultaneous Redundant GM Recovery

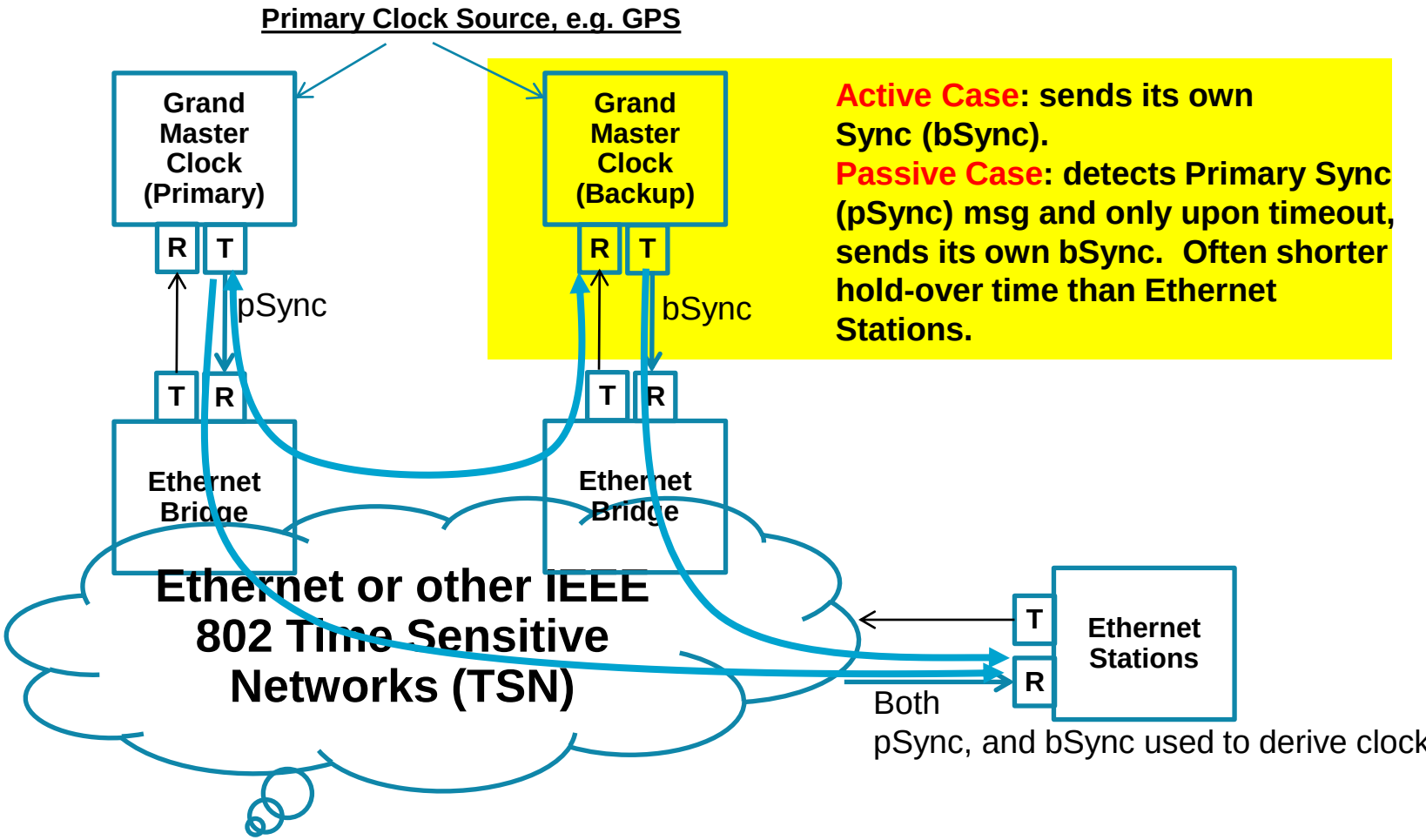
- Original pGM or a new GM is inserted into the network
  - Observation: new pGM (bGM) could have drifted far from the original pGM's clock reference
  - Previous pGM MUST synchronized to the pGM (original bGM).
  - Once synchronized the original pGM can become GM in event of failure
  - Active bGM: Upon detecting pGM, syntonize its clock to the pGM. It may optionally stop sending Sync (e.g. go to init state) while the change over from internal reference.
  - Passive: bGM stops sending Sync (after a pGM detection and some timeout).
  - pGM sends Sync and moves its synchronized clock to its own primary reference within jitter tolerance of apps specific MTIE (should be able get common lower bound).

Note: Due to pGM Heal-back operation, pGM also requires circuits to support synchronized clock.

- Device (e.g. Ethernet Station) Operation
  - Devices are not limited to Ethernet nodes, but all 802.1AS and 1588 capable network nodes.
  - Hold-over period is "entered" when no Sync is received – normal behavior. Hold-over period is when clock tolerance is within the operating specification for the use case when free-running (defined as no Sync received in expected period).
  - Functionally need not (not does not) distinguish pSync from bSync, and use both for synchronization and/or syntonization.
  - For reliability, specifically from protection from soft malfunction, 3 or more xSync could be received from 3 or more xGMs, and weighted selection (simple majority, weighted majority, etc) may be performed to qualify xSync before being used.
  - For reliability, specifically from protection from soft malfuction, each of the xSync is validated by expected range of time-value difference from the last respective xSync message before use. If out-of range time-value step is detected over a defined (configurable) time or sequence, the respective xGM may be deemed unreliable and may be signaled to network management entity.

Redundant Grandmaster Clock – Case 1

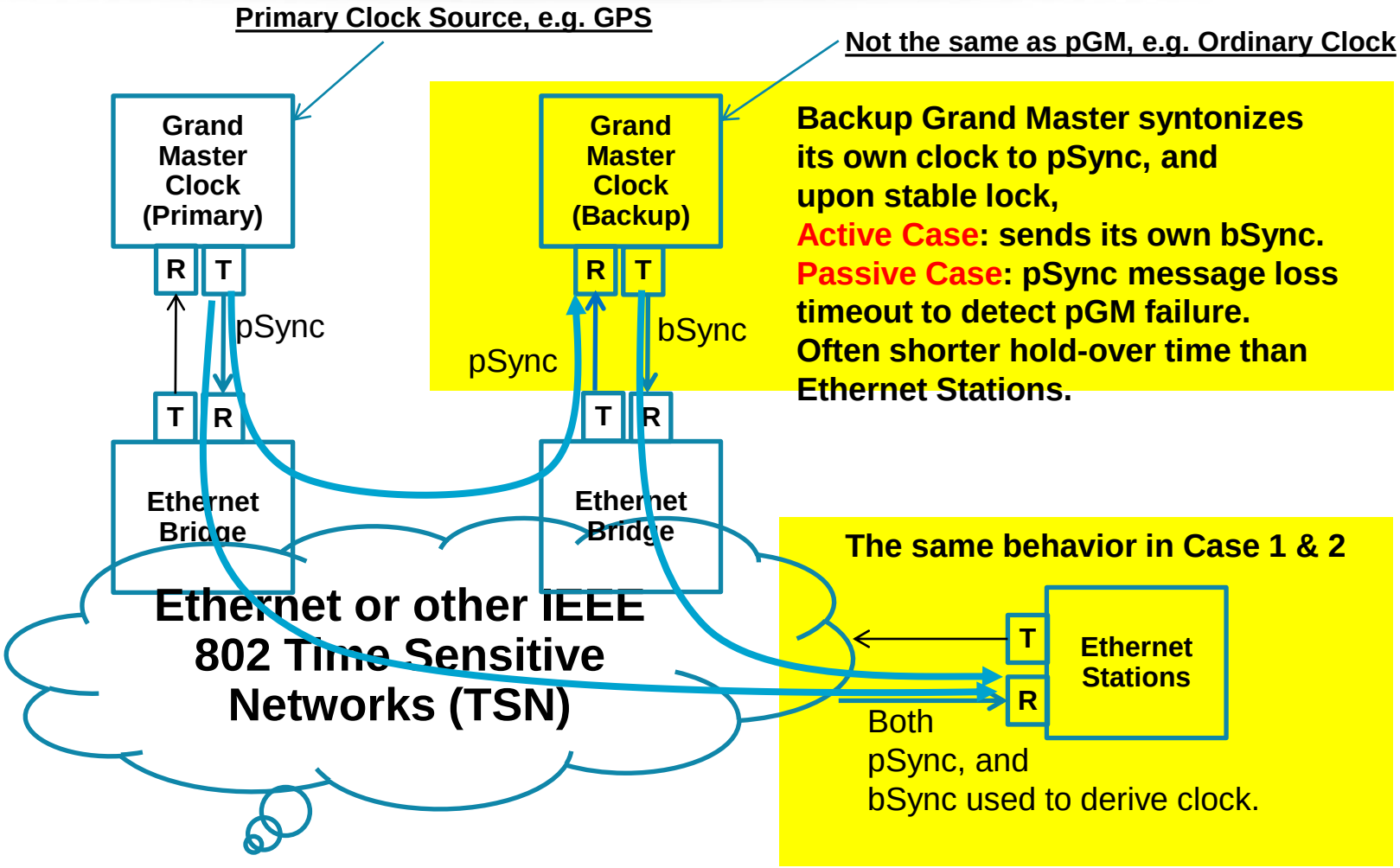
Operating



Case 1 – Primary and Backup Grand Masters have the same primary clock source

Redundant Grandmaster Clock – Case 2

Operating

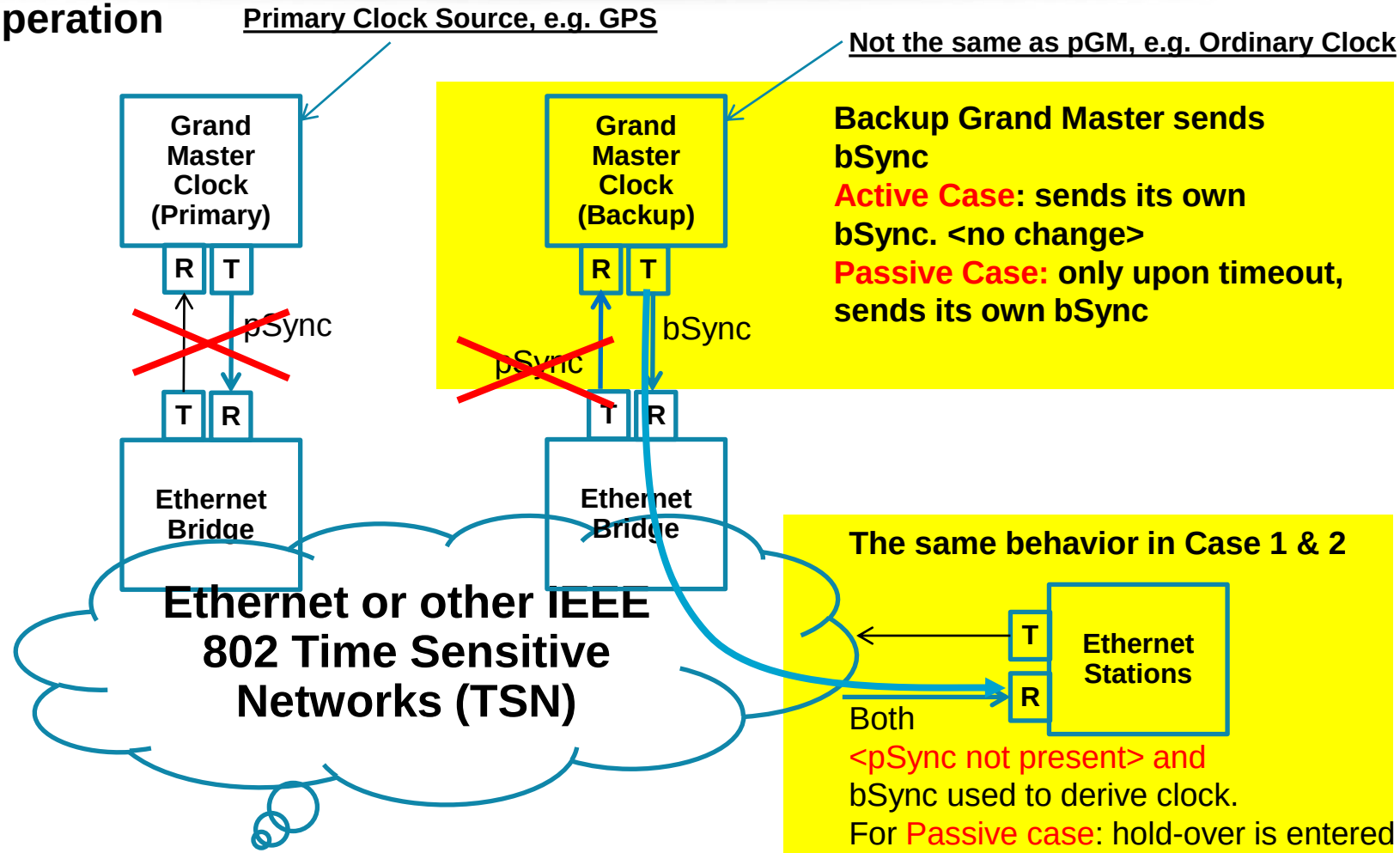


Case 2 – Backup and Primary Grand Master do not share the same clock source.

E.g. Primary has the preferred primary clock source, and Backup Grand Master has non-common clock as the primary, e.g. ordinary clock.

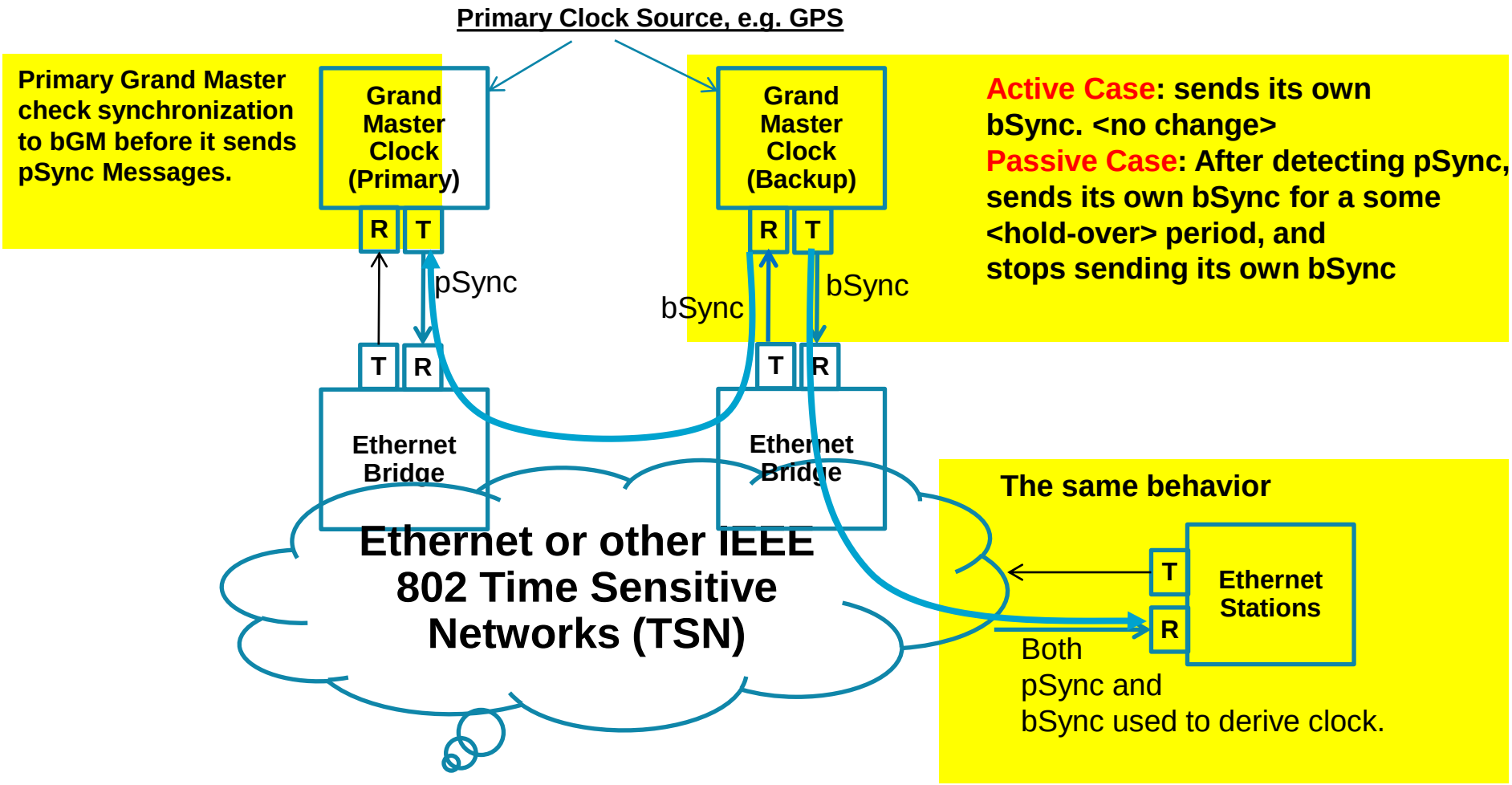
Redundant Grandmaster– Failed pGM

pGM Fail Operation



Common to Cases 1 & 2

Redundant Grandmaster– Healed pGM (Case 1)



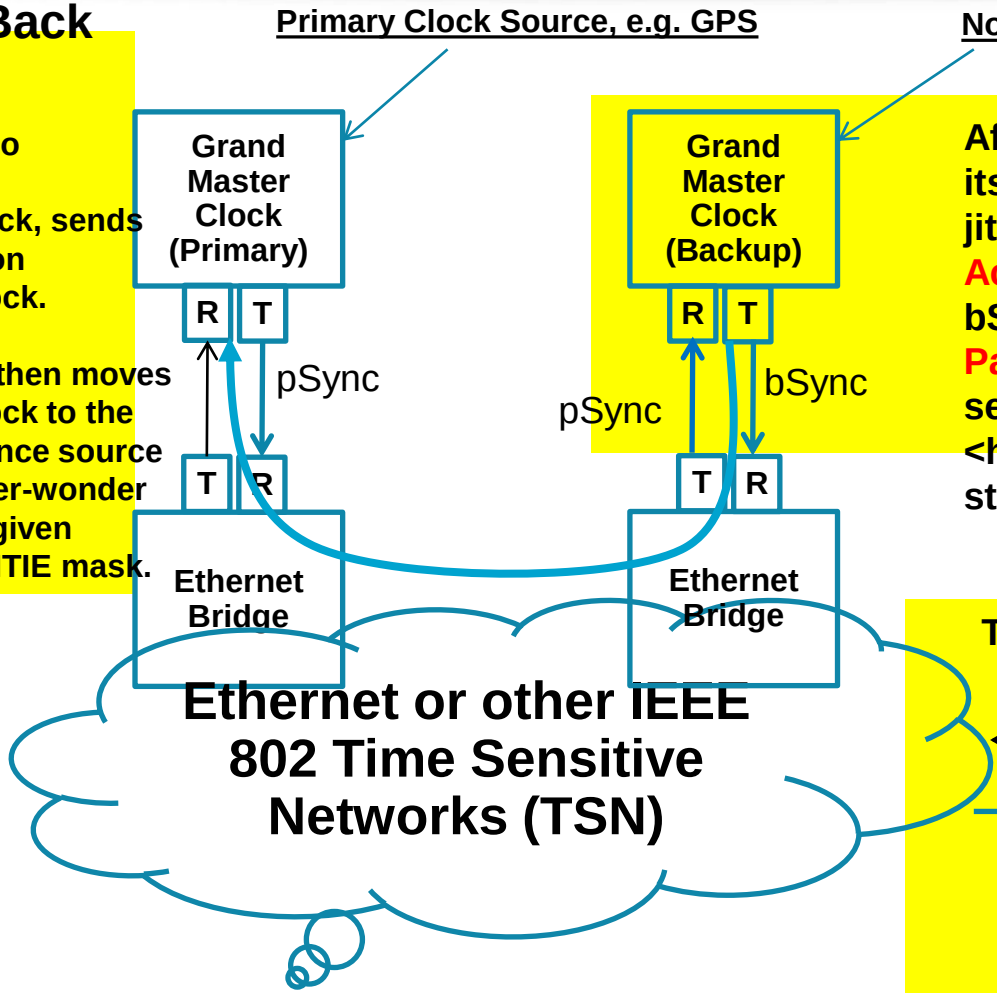
Case 1 – Primary and Backup Grand Masters have the same primary clock source

Redundant Grandmaster– Healed pGM (Case 2)

pGM Heal-Back

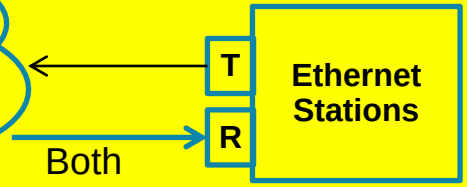
Grand Master syntonizes its own clock to bSync, and upon stable lock, sends pSync based on syntonized clock.

Grand Master then moves syntonized clock to the primary reference source by allowed jitter-wonder tolerance per given applications MTIE mask.



After detecting pSync, bGM syntonizes its clock to pSync within the same jitter-wonder tolerance as pGM.
Active Case: sends its own bSync. <no change>
Passive Case: After detecting pSync, sends it own bSync for a some <hold-over> period, and stops sending its own bSync

The same behavior



Both pSync and bSync used to derive clock.

Case 2 – Backup and Primary Grand Master do not share the same clock source.

Summary

- Timing Slave “could” behave the same in all cases – simpler behavior -- an objective in automotive.
- Passive backup GM switch-over time TBD – and perhaps local system minimum hold-over requirements.
- Three or more GM (or Four or more GM) allows for majority-check.
- Some end-points may participate in in-profile phase & frequency range check for each sync message (to help checking integrity).
- If found to be technically sound, propose to include in our work in 802.1ASbt.