Various Methods for Attaining a Resilient and Secure Timing Architecture

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

Eran Gilat
Manager, Systems Architecture

Agenda

1. Resilient Global BMCA
2. Majority Vote Algorithm
3. Systems Redundancy Schemes
4. Summary

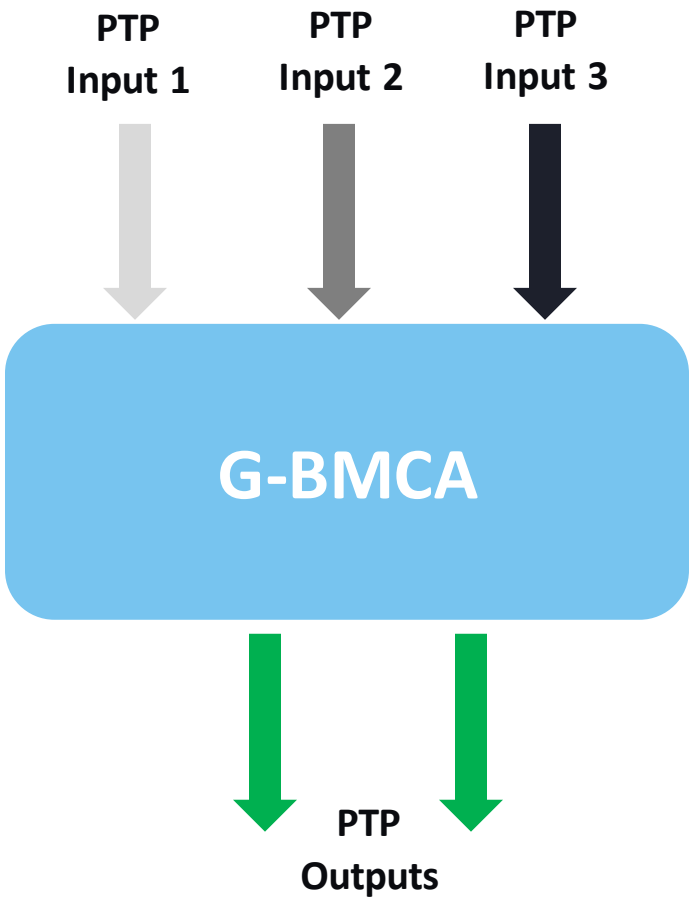
Resilient Global BMCA (G-BMCA) Algorithm

IEEE 1588 Definition:

The best master clock algorithm specifies the way that a PTP Instance determines which of all the PTP Instances (including itself) is the “best”

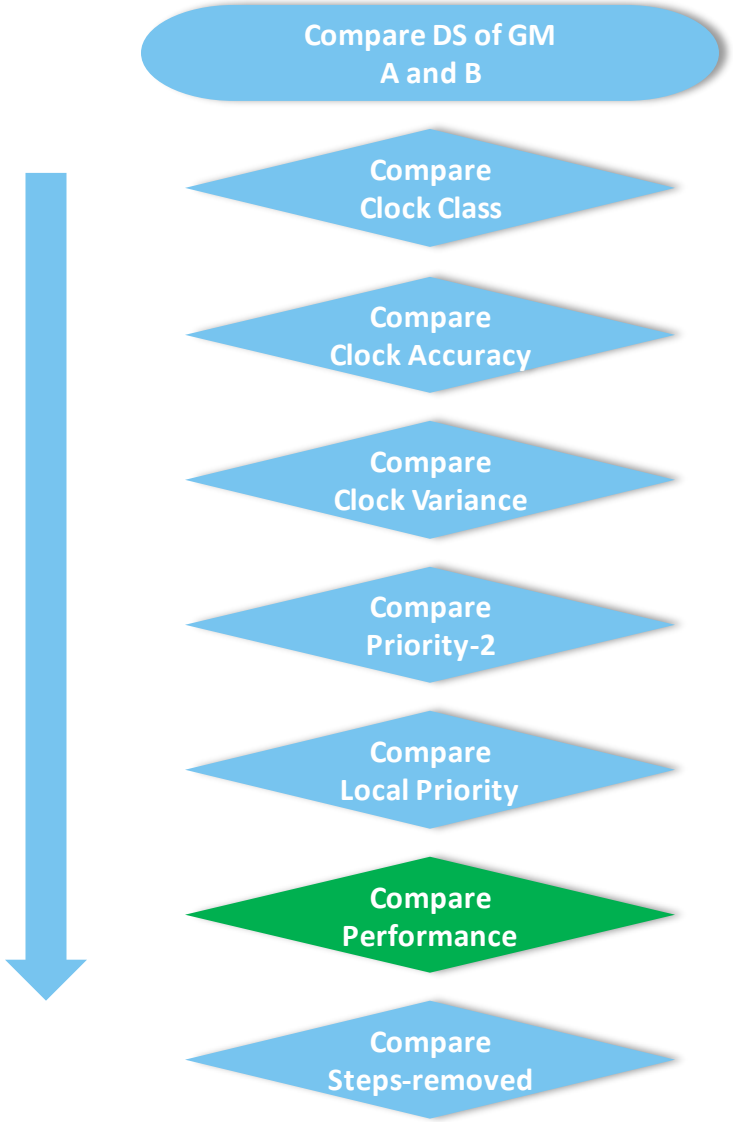
Advantages of G-BMCA

- G-BMCA is an extension to the standard/alternate BMCA defined by IEEE 1588 and ITU-T standards Committee
- Standard/alternate BMCA assume a single profile. G-BMCA can run with a mix of profiles using a mapping function of the various PTP parameters
- In addition to the data set comparison, G-BMCA includes the comparison of PTP performance using a “Figure of Merit” metric
- G-BMCA has the option to run on multiple clock domains to support parallel paths of synchronization (i.e., east/west domains) to protect against reference/path failures



MICROCHIP

Resilient Global BMCA Advantages

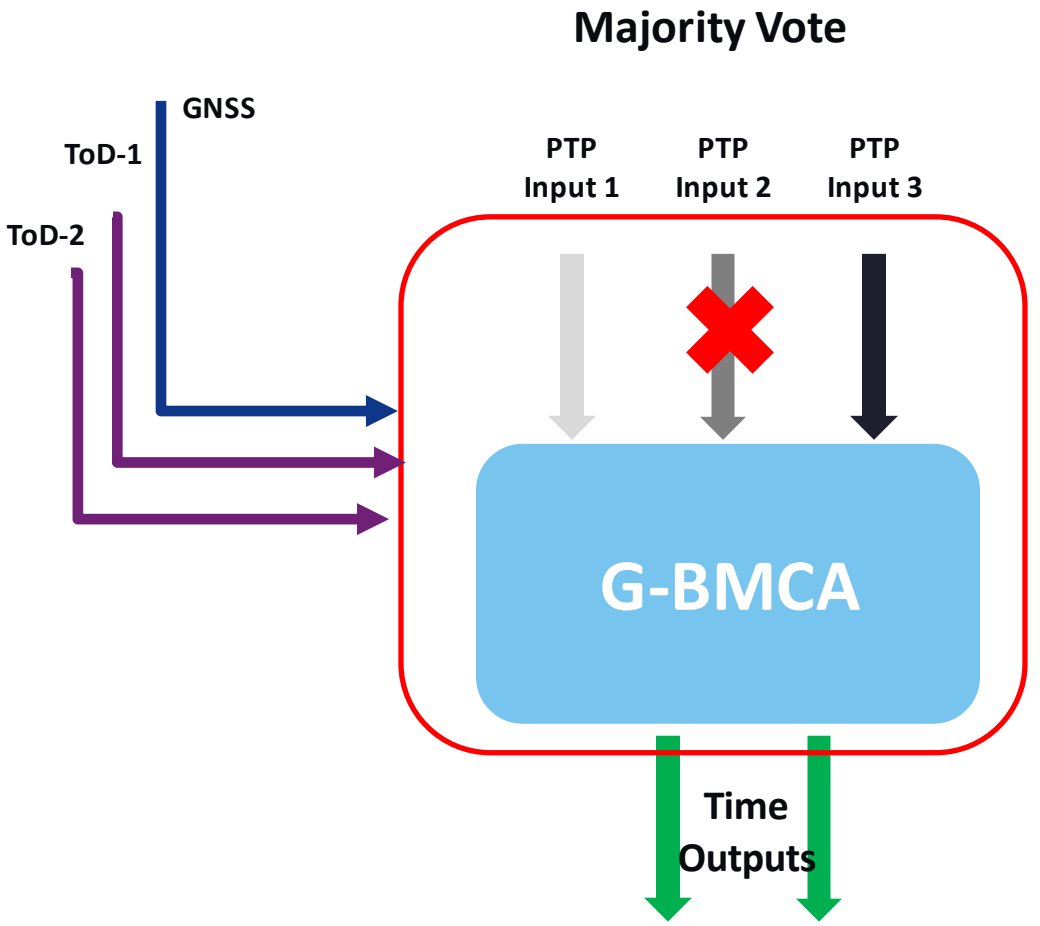


- Ability to turn on/off “Performance” check
- Conservative location of the “Performance” check in the G-BMCA chain
- Future enhancements will include the ability to move the “Performance” check anywhere in the BMCA chain

MICROCHIP

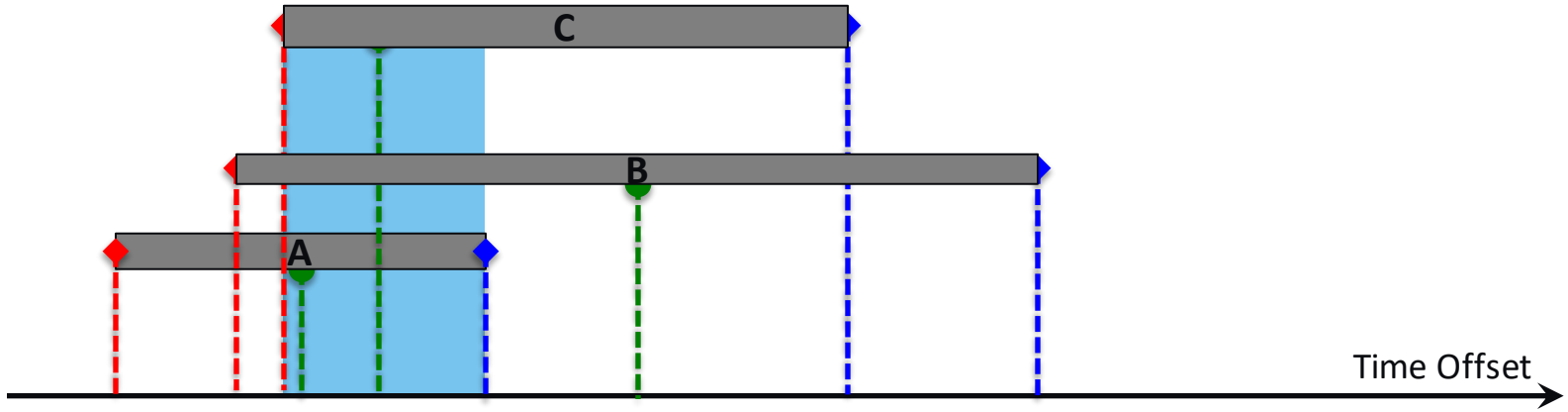
Majority Vote Algorithm Essentials

- **Why?**
  - Security - spoofing attacks
  - Resiliency - unintentional clock errors
- **What?**
  - Prior to the G-BMCA decision tree, Majority Vote (MV) can exclude any 1 of 3 time references
  - MV determines if there are any outliers and rejects them
- **Supported Combinations:**
  - Three instances of PTP clients on the same system
  - Two instances of PTP clients plus GNSS time reference
  - Two instances of PTP clients plus G.8271 ToD time reference



Majority Vote Algorithm–How?

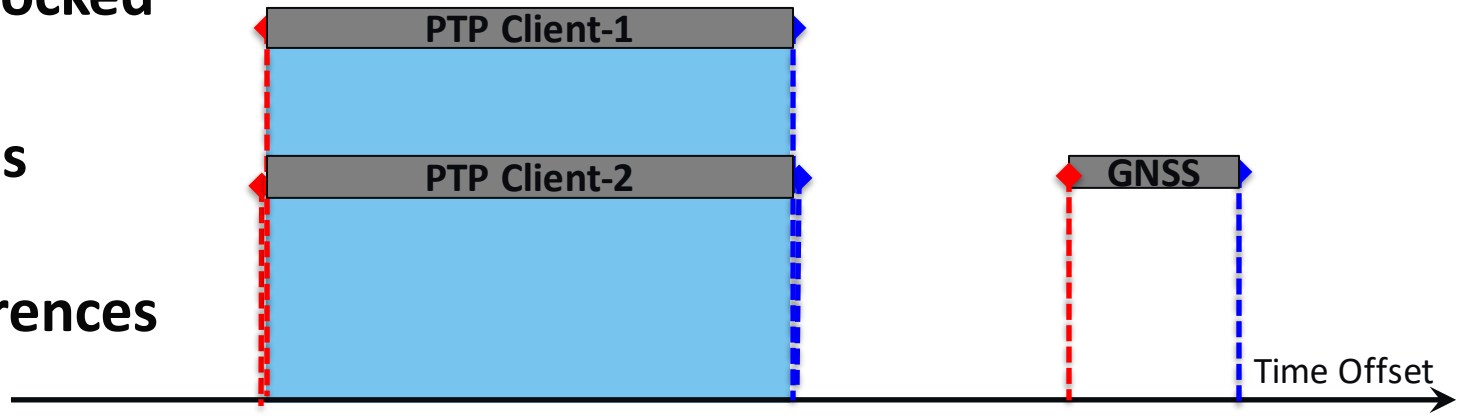
- Time offsets are calculated based on a single reference point
- User defined threshold to determine correctness intervals
- Dynamic adjustment of correctness intervals for hysteresis
- Use a common algorithm to locate “Intersection Interval”
- A change in state (reject or valid) will need to persist for few seconds before the change is reported



Example 1: Intersection of 3 clocks, all clocks are valid

Example 1–One Clock Outlier

- Unit Under Test (UUT) is initially locked to GNSS reference
- Industry standard testing device is added into the scenario injecting arbitrary time with dual PTP references
- UUT rejects the higher priority reference (GNSS)




```
System Date and Time                    : 2021-10-08 02:00:32
  Clock Time Status                     : LOCKED
  Currently Selected Time Reference     : PTP Client (PI-1)
  Time State Duration (min)             : 44
  Clock Frequency Status                : LOCKED
  Currently Selected Frequency Reference : PTP Client (PI-1)
  Frequency State Duration (min)        : 48
  System Uptime                         : 0 day(s) 1 hour(s) 7 minute(s)
4 second(s)
Timing Service Eth7 Mode                : PTP Client (PI-0)
  Timing Service Eth8 Mode              : PTP Client (PI-1)
  Timing Service Exp Mode               : NONE
  Active Management Interface           : ETH1
  Redundancy Mode Status                : Stand-alone
  Frequency Stability (MDEV ppb)        : 0.114922
  Phase Stability (TDEV ns)             : 47.772
  Active Alarms                         : 12
  System Frequency PQL                  : 2
  Operation Mode                        : gateway-clock
  Last Config Time                      : 2021-10-10 05:25:29
  System Status                         : ok
```

Alarm Status

ID	Severity	Date-Time	Description
242	MINOR	2021-10-08 03:10:20	GNSS input reference majority vote rejection

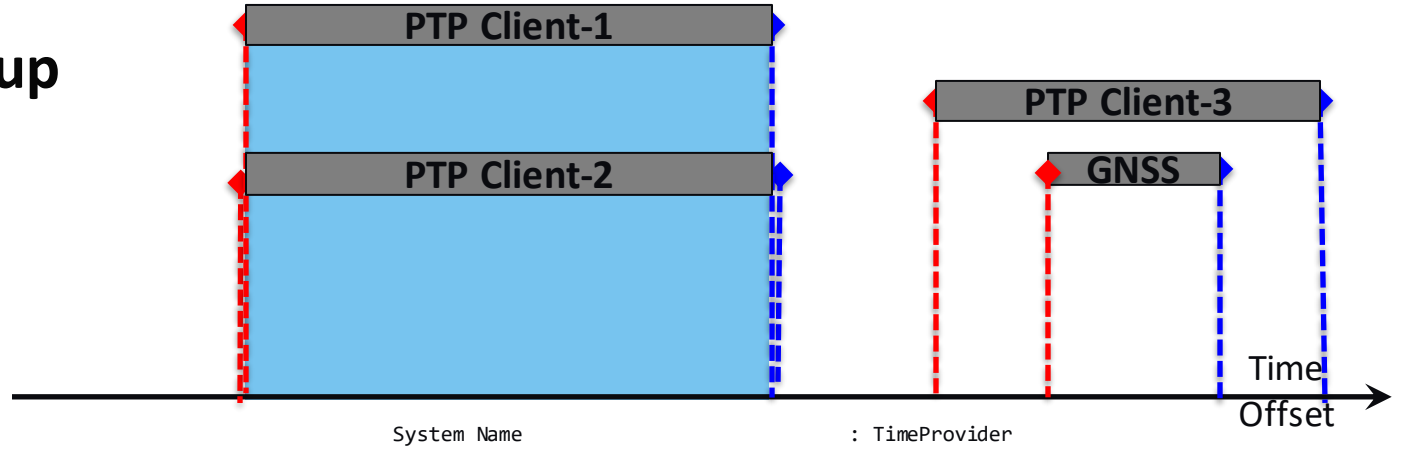
Majority Vote Status

Reference	status
GNSS	reject
PTP (PI-0)	valid
PTP (PI-1)	valid
PTP (PI-2)	not-used

MICROCHIP

Example 2–No Overlap

- Third PTP reference sourced from House Time Scale is added to the setup
- There is no intersection, therefore majority vote cannot be determined. All clocks are marked valid
- Higher priority was set to the GNSS input which is now selected as system reference




```
Reference Criteria                    : priority
Reference Switch Mode                 : auto-return


Operation Mode                        : gateway-clock
Majority-Vote Mode                    : enable
Majority-Vote Threshold               : 1000 ns

Time Reference Config
```

Reference	Priority
GNSS	1
PTP	2
TOD-1	4
TOD-2	4

Majority Vote Status

Reference	status
GNSS	valid
PTP (PI-0)	valid
PTP (PI-1)	valid
PTP (PI-2)	valid
TOD-1	not-used
TOD-2	not-used

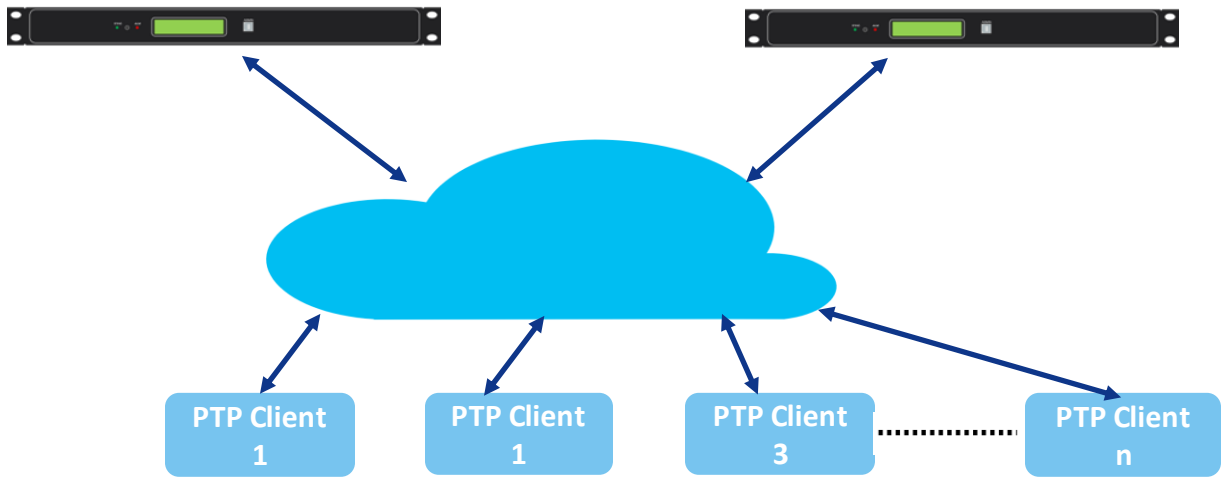
```
System Name                           : TimeProvider
  Serial Number                       : SCA20070010F
  System Date and Time                : 2021-10-10 21:25:50
  Clock Time Status                   : LOCKED
  Currently Selected Time Reference   : GNSS
  Time State Duration (min)           : 832
  Clock Frequency Status              : LOCKED
  Currently Selected Frequency Reference : GNSS
  Frequency State Duration (min)      : 832
  System Uptime                       : 0 day(s) 14 hour(s) 42
minute(s) 45 second(s)
  Timing Service Eth1 Mode            : NONE
  Timing Service Eth2 Mode            : NONE
  Timing Service Eth3 Mode            : NONE
  Timing Service Eth4 Mode            : NONE
  Timing Service Eth5 Mode            : PTP Client (PI-2)
  Timing Service Eth6 Mode            : NONE
  Timing Service Eth7 Mode            : PTP Client (PI-0)
  Timing Service Eth8 Mode            : PTP Client (PI-1)
  Timing Service Exp Mode             : NONE
  Active Management Interface         : ETH1
  Redundancy Mode Status              : Stand-alone
  Frequency Stability (MDEV ppb)      : 0.007607
  Phase Stability (TDEV ns)           : 3.162
  Active Alarms                       : 0
  System Frequency PQL                : 1
  Operation Mode                      : gateway-clock
  Last Config Time                    : 2021-10-08 04:07:24
  System Status                       : ok
```


MICROCHIP

Introduction of Various Redundancy Schemes

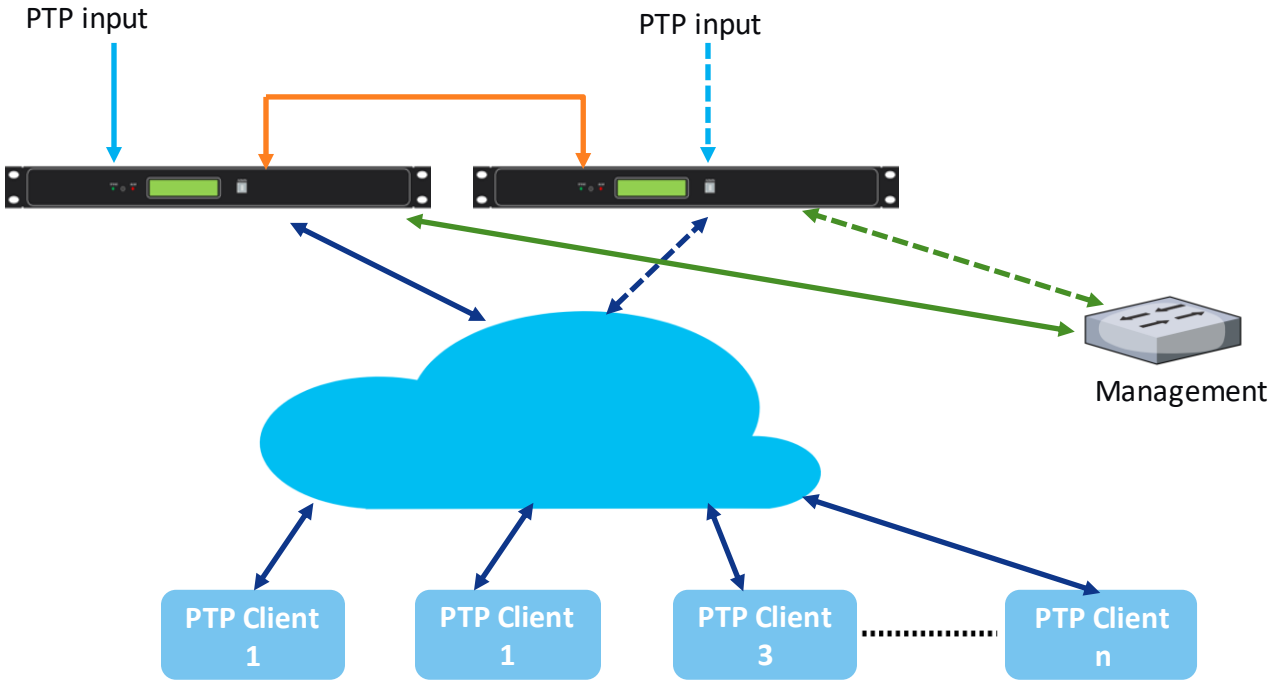
Geographical Redundancy/Network Redundancy

- Two or more PTP server units are deployed in separate locations in the network, same profile and same domain
- According to BMCA or A-BMCA: PTP clients will connect to the lower priority GM in case of a fail-over scenario or attributes degradation
- PTP server units are not synchronized and are not configured similarly. This is a plain fail-over network redundancy



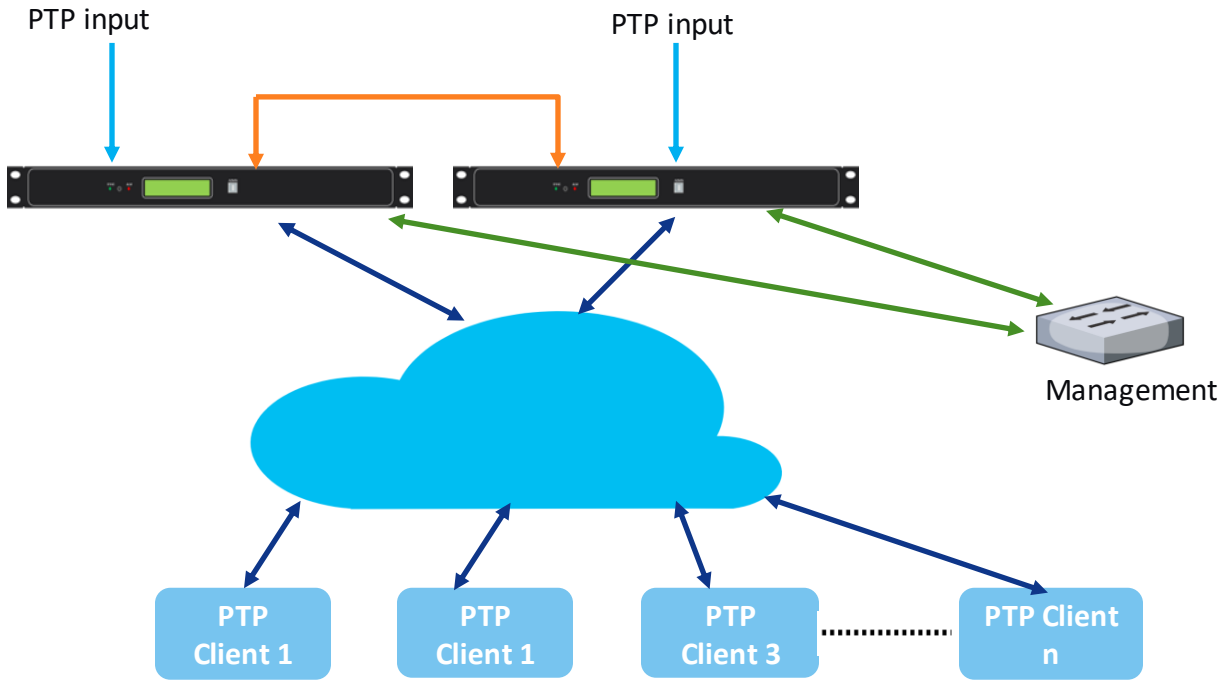
Active Standby Redundancy

- **“Hardware Redundancy” achieved by using either:**
  - Two identical units, one is active, the other is standby
  - Single redundant device with redundant clock modules
- **Behavior is essentially as a single unit**
- **Out-of-Band channel for sync and management between redundant Hardware units**
- **Both units have unified configuration, including software options**
- **Unified PTP client list transferred via OOB channel**
- **The two devices “look” like a single unit for all practical purposes and share the same GM Clock ID.**
- **Unit management is only live for active units in case of dual hardware or is single connected via a non-redundant management module**
- **PTP input is operative only on active units**



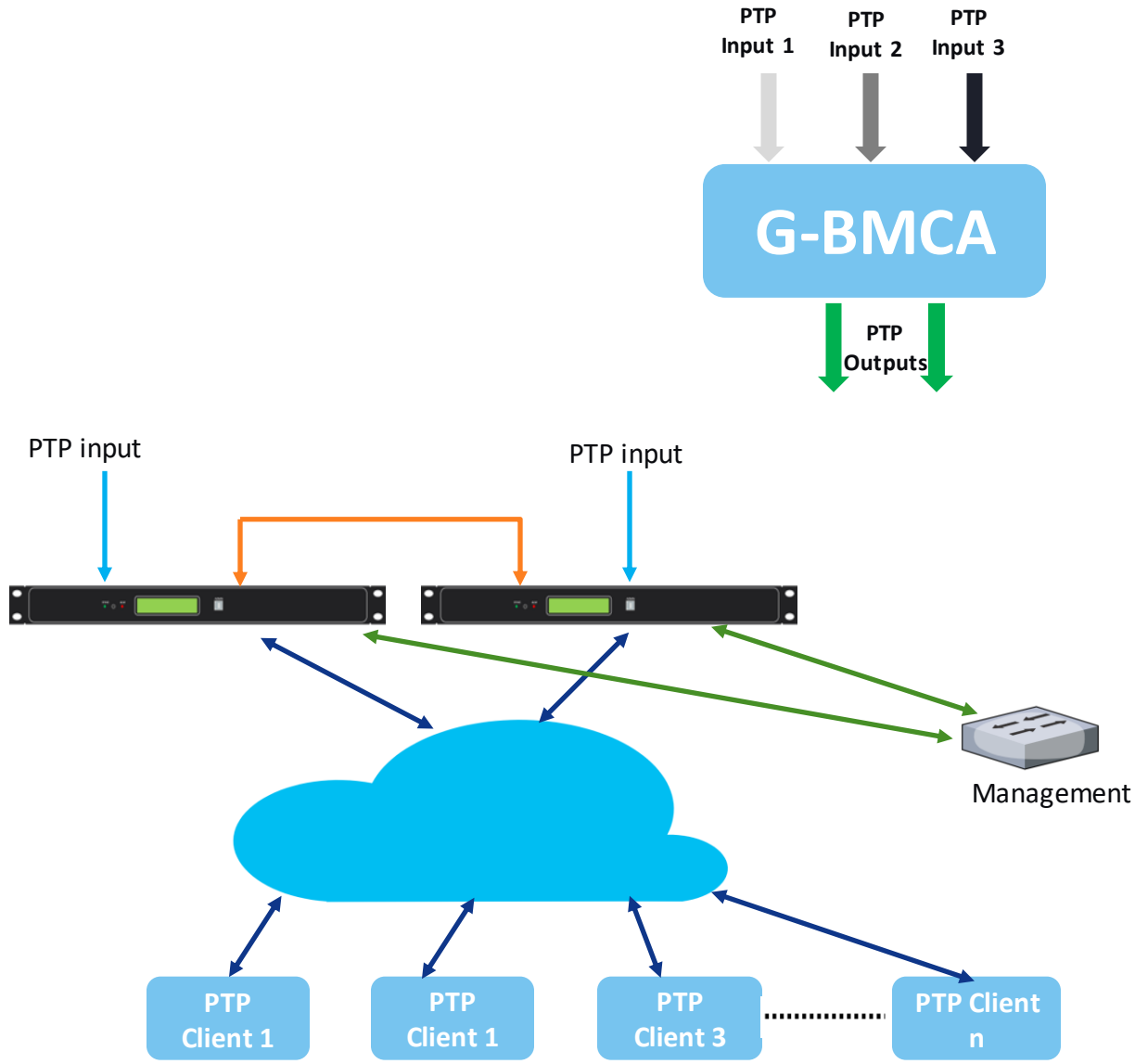
Active-Active Redundancy

- Two separate devices act as two separate GMs with Common Time Base
- Out of Band (OOB) channel is only for sync, not management
- Management is active on both units
- The two units are not necessarily configured similarly
- Much more flexibility but also potential risks for configuration errors
- PTP input or inputs available and active on both active units at the same time
- BMCA with Health status methods are used as arbitration method to determine SyncSender and SyncReceiver roles.



Active-Active Redundancy (Contd.)

- **Active-Active redundancy is an extension of G-BMCA and Majority Vote features into hardware redundant platform**
- **Determination of SyncSender and SyncReceiver roles takes advantage of either or both capabilities**
- **Active-Active variant of redundancy allows support of additional architectures and use cases:**
  - Redundant SSU with Frequency only inputs
  - vPRTC with mesh DWDM optical networks



Summary

- There is a growing need in the industry to assure selected timing sources are valid and that the content isn't spoofed or modified
- IEEE 1588-2019 standard, under Security Annex P, introduced in Prong C Guidance to address security and resilience with architecture methods as described in this presentation
- The use of techniques such as Global BMCA and Majority Vote are some of the methods being developed to ensure resilience timing performance
- The Active-Active redundancy scheme is used to extend the reach of those techniques to support even more resiliency using 1:1 hardware redundancy

Thank you

Eran Gilat

Manager, Systems Architecture

Eran.Gilat@microchip.com

Phone: +1-408-964-7671

MICROCHIP