Discussion of Time Sync Redundancy

Rodney Greenstreet, Rodney Cummings
National Instruments

NATIONAL INSTRUMENTS

Motivation for Redundant Time Sync

- GM and path redundancy provides:
  - Fault tolerance
  - Integrity
  - Security
- Industries
  - Industrial control
  - Automotive
  - Financial
  - …

Proposed Road Map

1. Define and agree on assumptions
2. Create a new PAR
   - Assumption: Not addressed in 802.1AS rev
3. Specify technical details for the PAR

- This presentation is the beginning of step 1

Review Modes of Failure

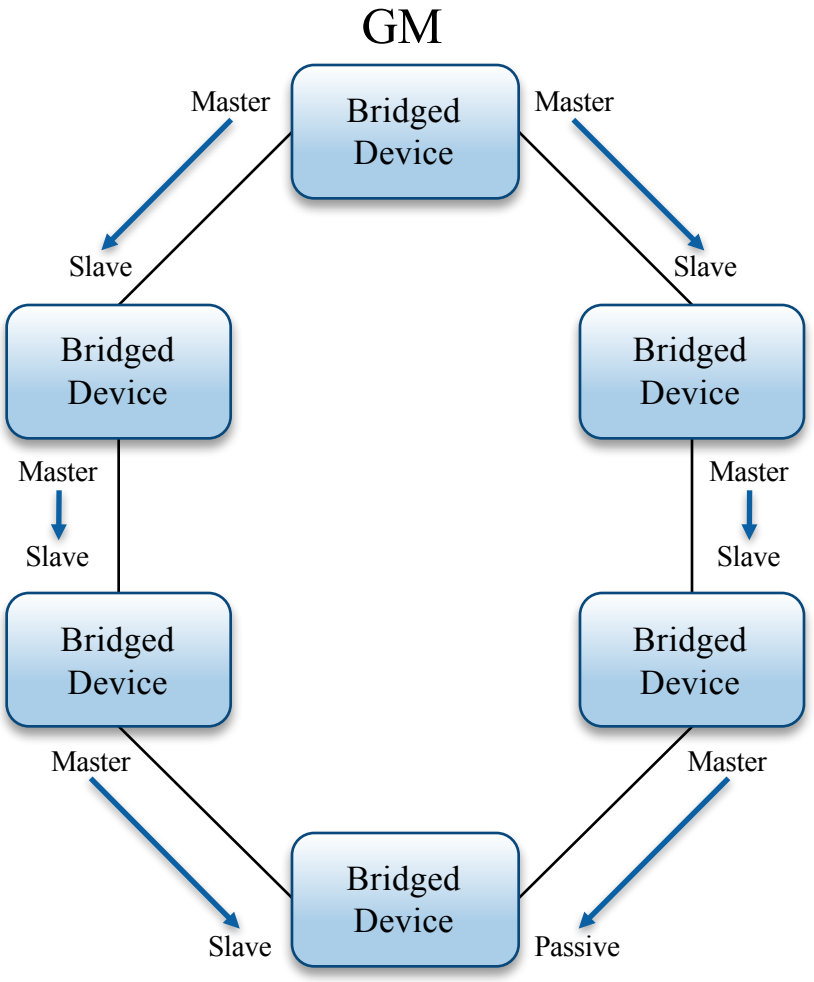
Failure Concepts

- Single-failure: At most one device
  - Device = End station, bridge/router, or link between
    - Including GM clock failure
- Dual-failure: At most two devices
- Failure modes: How
  - Fail-silent: Device stops transferring time
  - Fail-consistent: Send faulty time, but same to all receivers
  - Fail-inconsistent: Different time to each receiver (byzantine)
    - NASA – Real System Failures
- Failure modes: When
  - Permanent: Device unable to recover (i.e. offline until replaced)
  - Transient: Fault comes and goes (e.g. omit some frames)
- Multipath synchronization: Provides failover of time synchronization through redundant physical paths
- Multi-clocks: Provides failover of time synchronization through redundant GM's

Redundancy Examples using Ring Topology

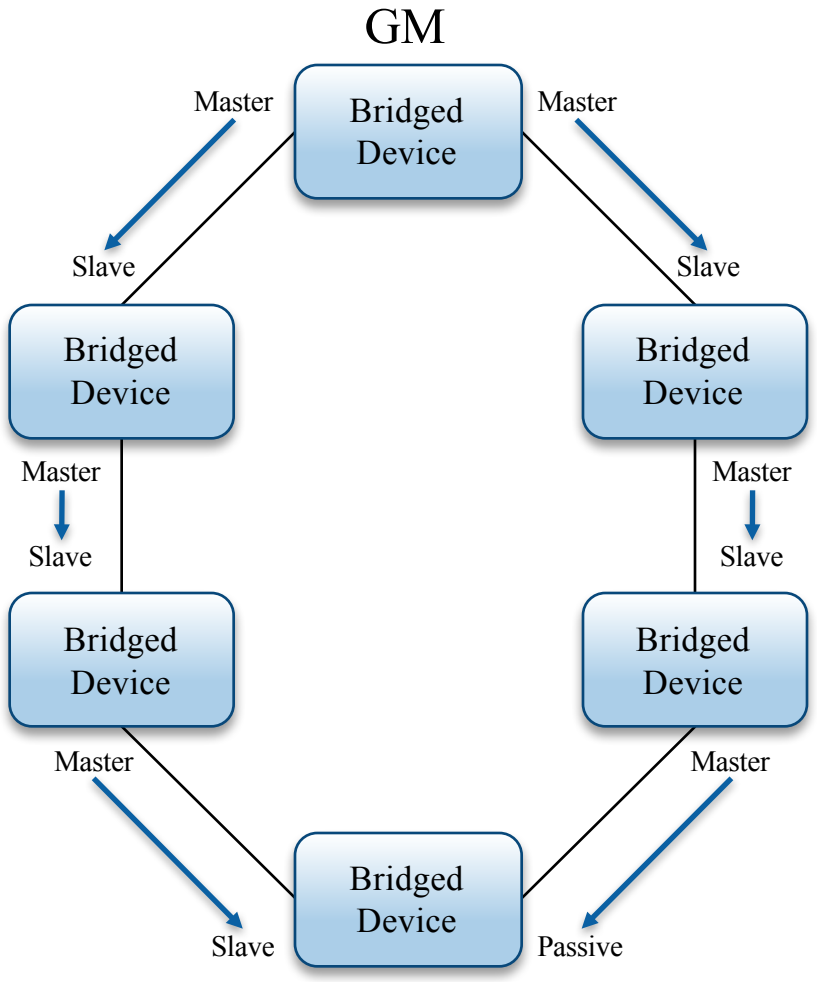
Redundancy using BMCA

- Advantages:
  - Already in standard
  - Addresses path failures
  - Addresses ‘fail-silent’



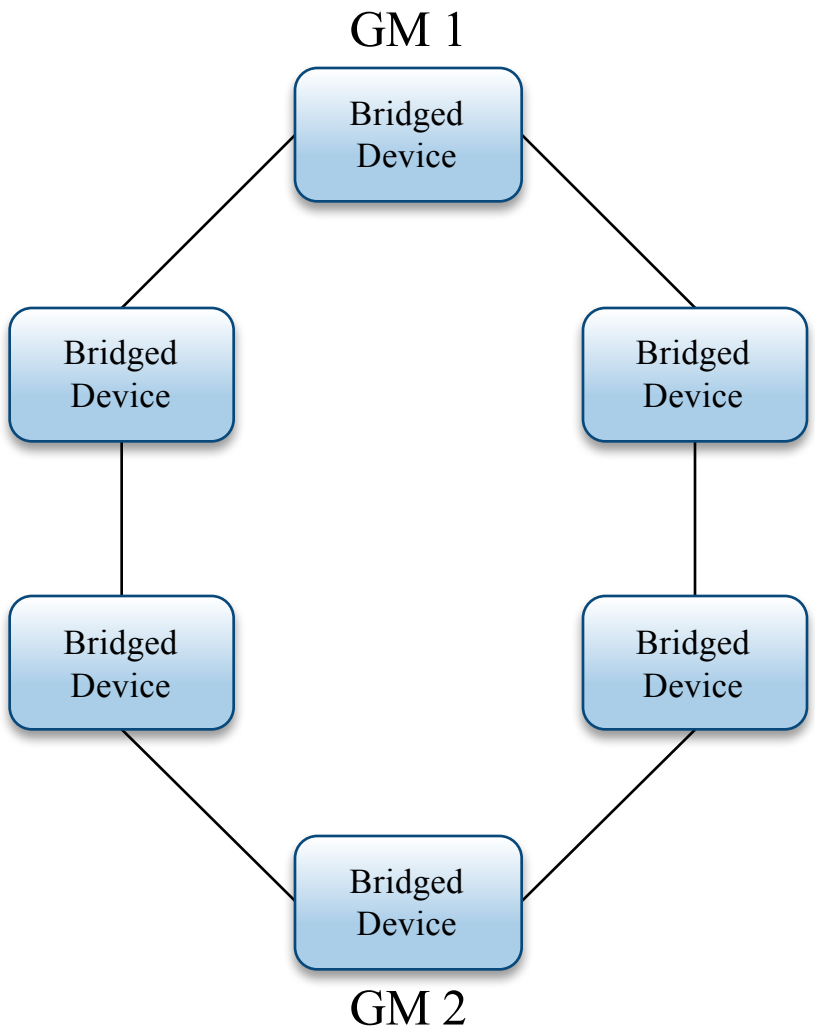
Redundancy using BMCA

- Advantages:
  - Already in standard
  - Addresses path failures
  - Addresses ‘fail-silent’
- Disadvantages:
  - Does not address engineered networks
  - Path failures and ‘fail-silent’ are not seamless
    - Some applications may require holdover or increased traffic
  - Does not address ‘fail-consistent’
  - Does not address ‘fail-inconsistent (byzantine)’



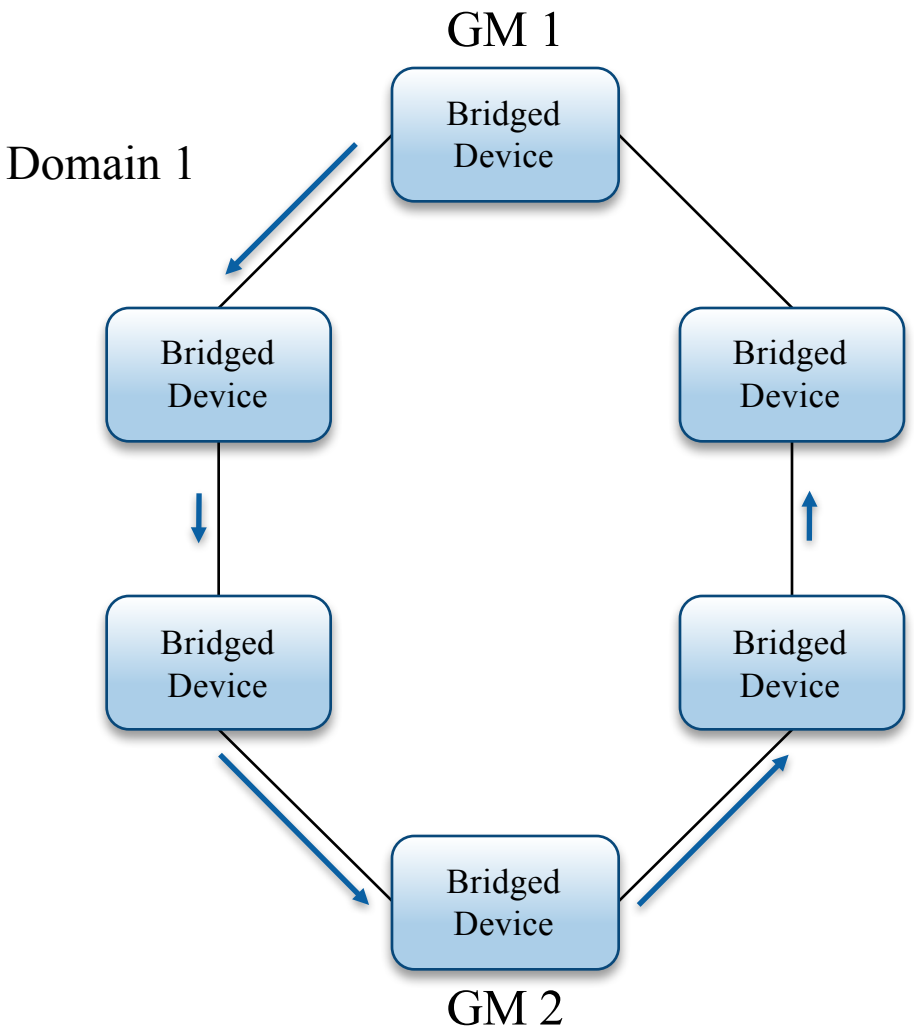
Redundancy with 2 GM's

- Observations:
  - Requires 4 domains
    - Seamless path failure requires at least 2 domains per GM (multipath)



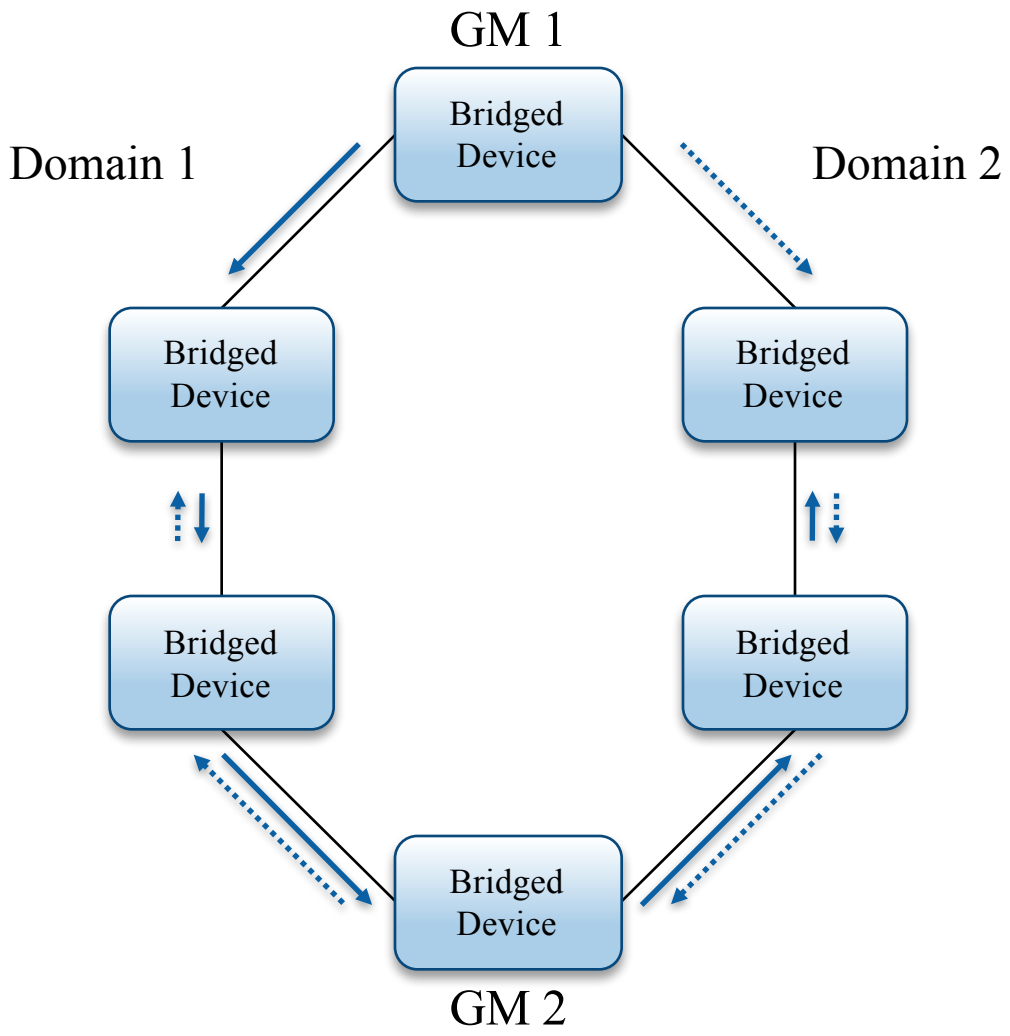
Redundancy with 2 GM's

- Observations:
  - Requires 4 domains
    - Seamless path failure requires at least 2 domains per GM (multipath)



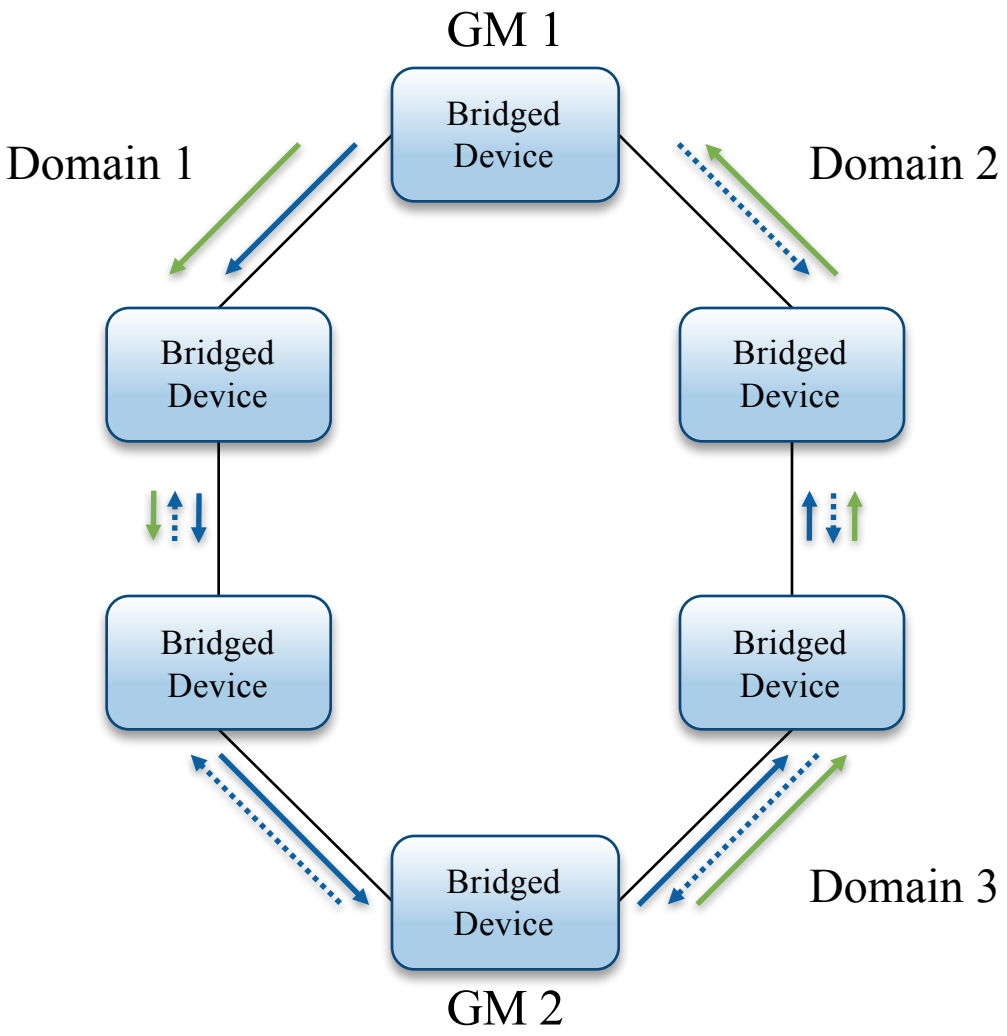
Redundancy with 2 GM's

- Observations:
  - Requires 4 domains
    - Seamless path failure requires at least 2 domains per GM (multipath)



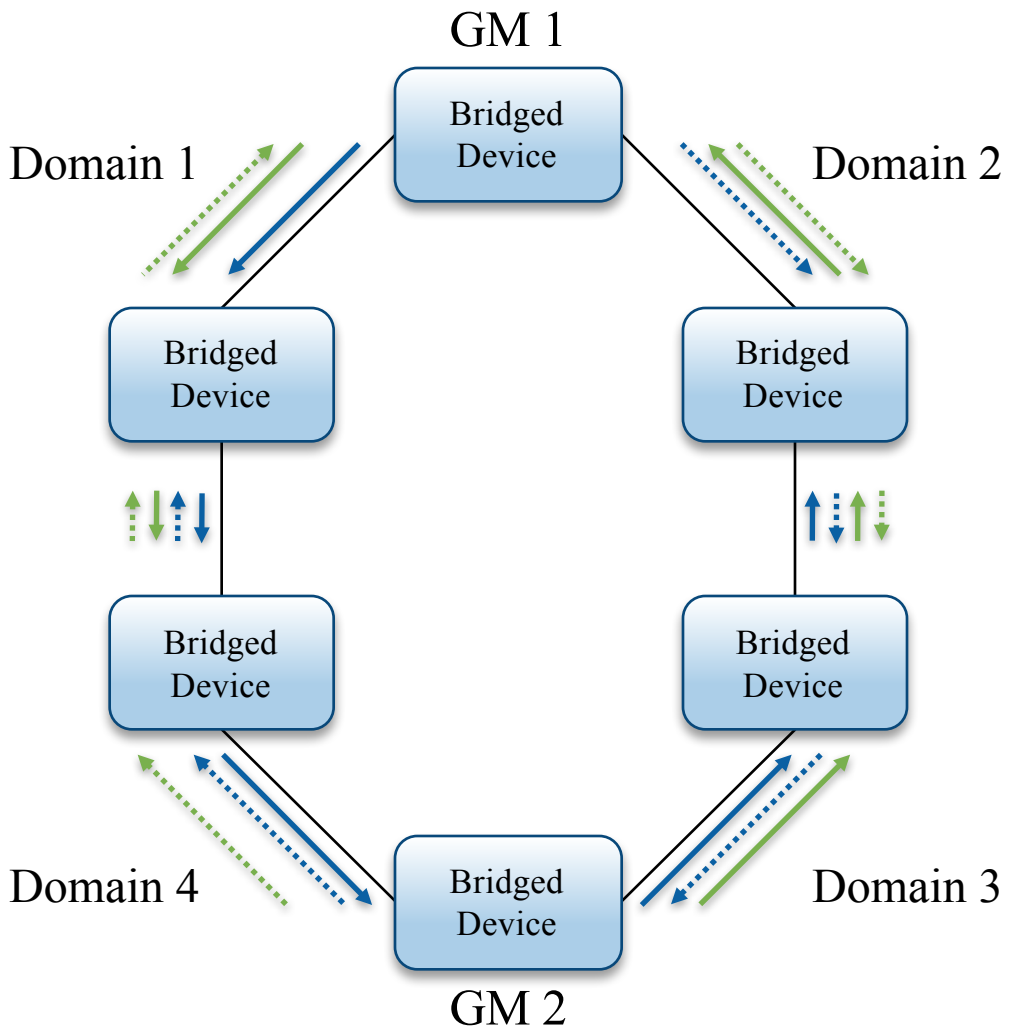
Redundancy with 2 GM's

- Observations:
  - Requires 4 domains
    - Seamless path failure requires at least 2 domains per GM (multipath)



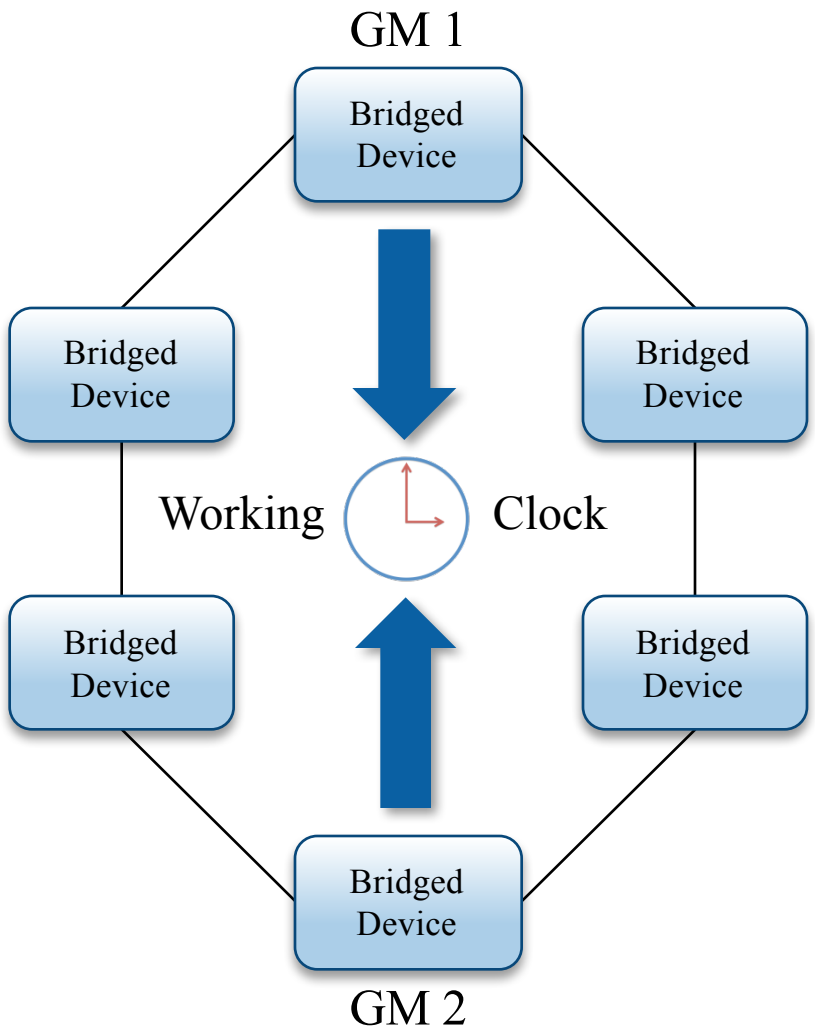
Redundancy with 2 GM's

- Observations:
  - Requires 4 domains
    - Seamless path failure requires at least 2 domains per GM (multipath)



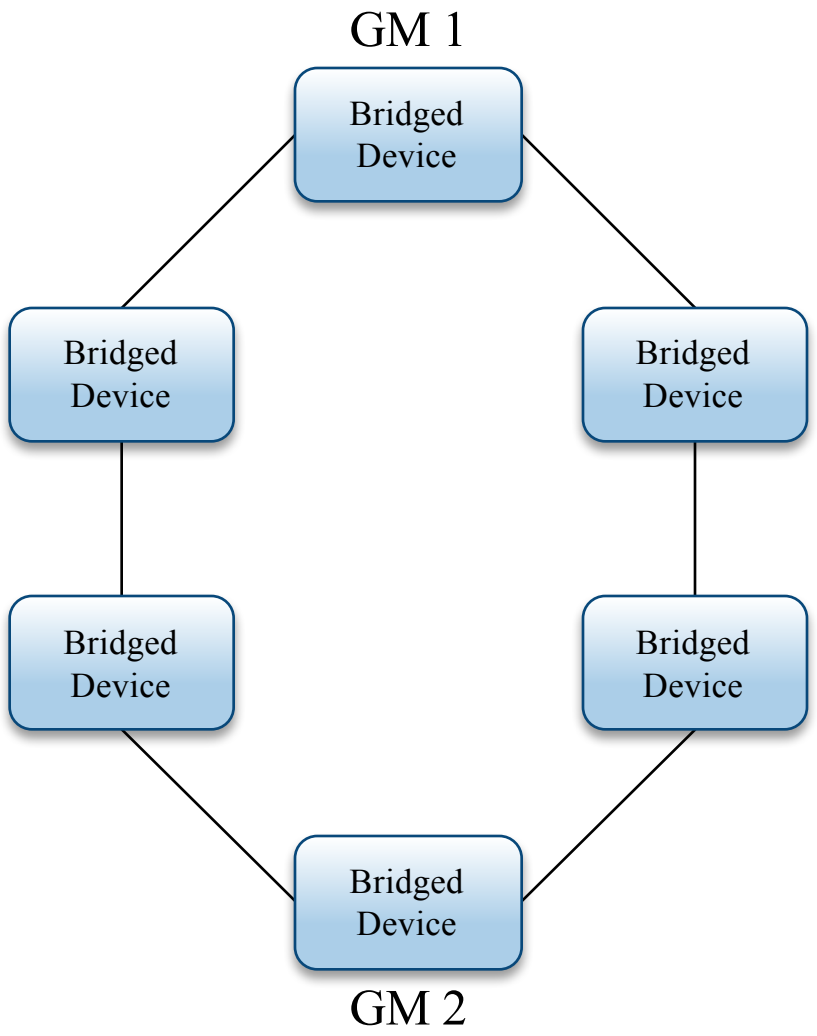
Redundancy with 2 GM's

- Observations:
  - Requires 4 domains
    - Seamless path failure requires at least 2 domains per GM (multipath)
  - Requires convergence of time between GM's
    - Prevents phase shift during faults



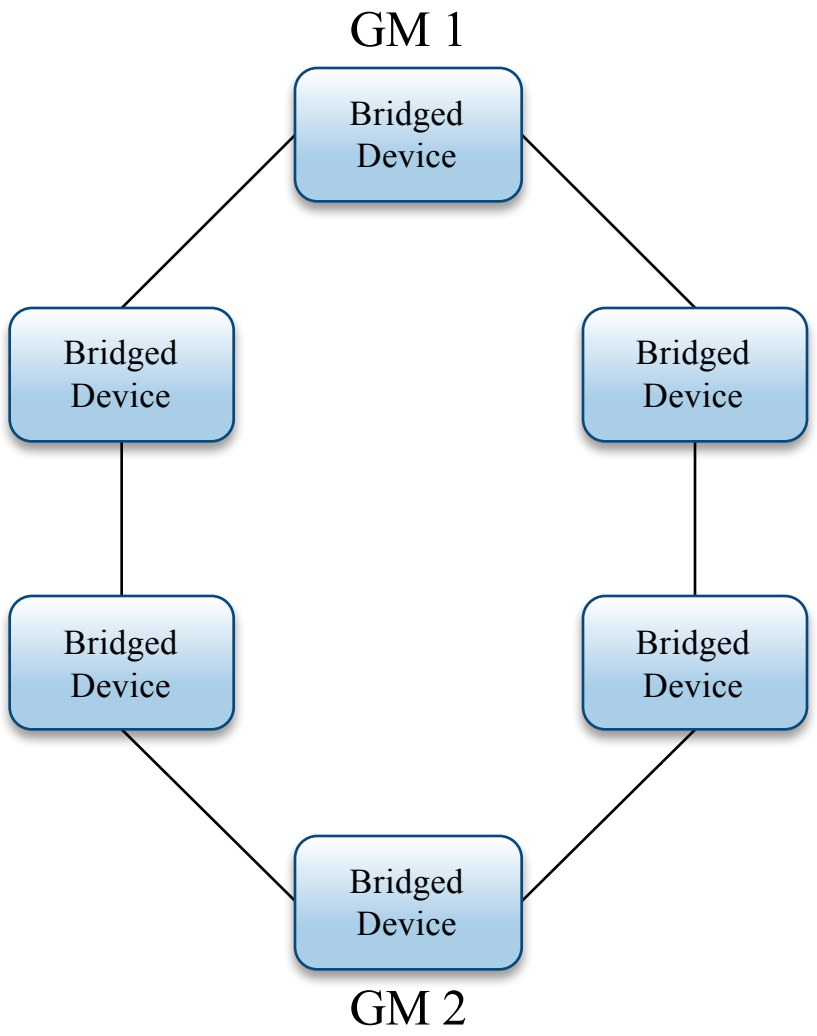
Redundancy with 2 GM's

- Observations:
  - Requires 4 domains
    - Seamless path failure requires at least 2 domains per GM (multipath)
  - Requires convergence of time between GM's
    - Prevents phase shift during faults
- Advantages:
  - Addresses engineered networks
  - Addresses seamless path failures
  - Addresses seamless 'fail-silent'



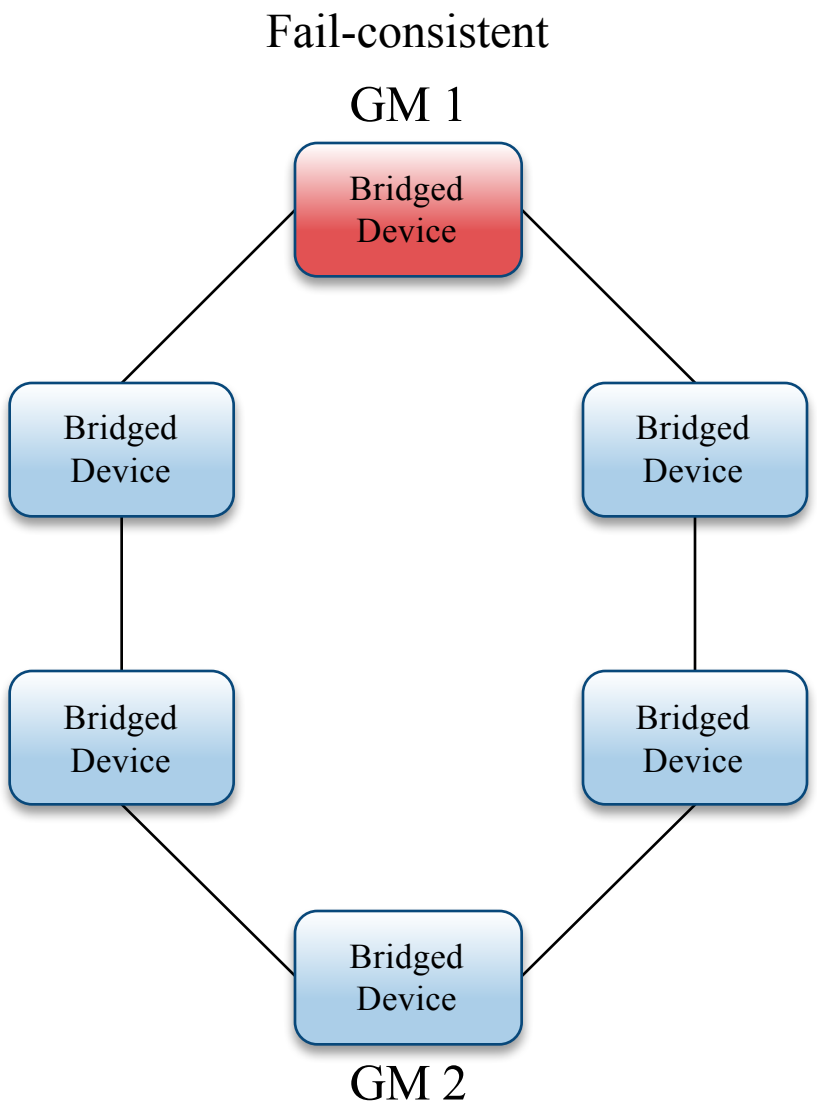
Redundancy with 2 GM's

- Observations:
  - Requires 4 domains
    - Seamless path failure requires at least 2 domains per GM (multipath)
  - Requires convergence of time between GM's
    - Prevents phase shift during faults
- Advantages:
  - Addresses engineered networks
  - Addresses seamless path failures
  - Addresses seamless 'fail-silent'
- Disadvantages:
  - Does not address 'fail-consistent'



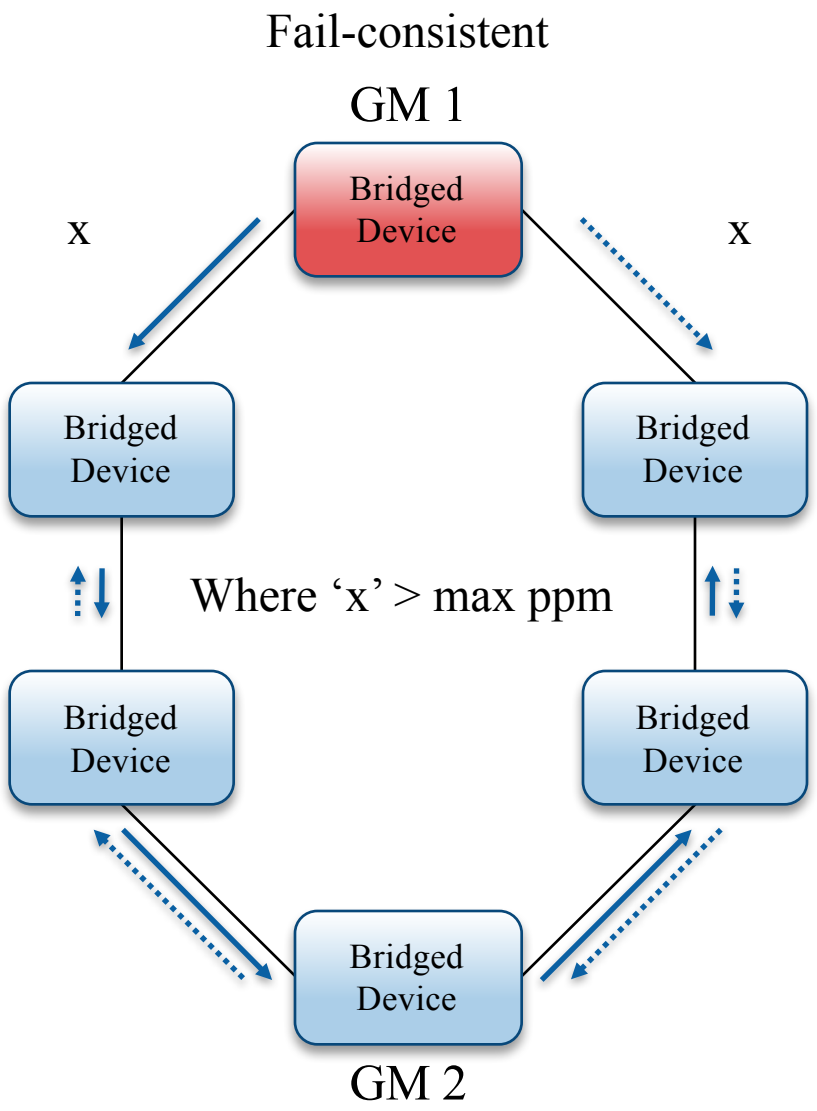
Redundancy with 2 GM's

- Observations:
  - Requires 4 domains
    - Seamless path failure requires at least 2 domains per GM (multipath)
  - Requires convergence of time between GM's
    - Prevents phase shift during faults
- Advantages:
  - Addresses engineered networks
  - Addresses seamless path failures
  - Addresses seamless 'fail-silent'
- Disadvantages:
  - Does not address 'fail-consistent'



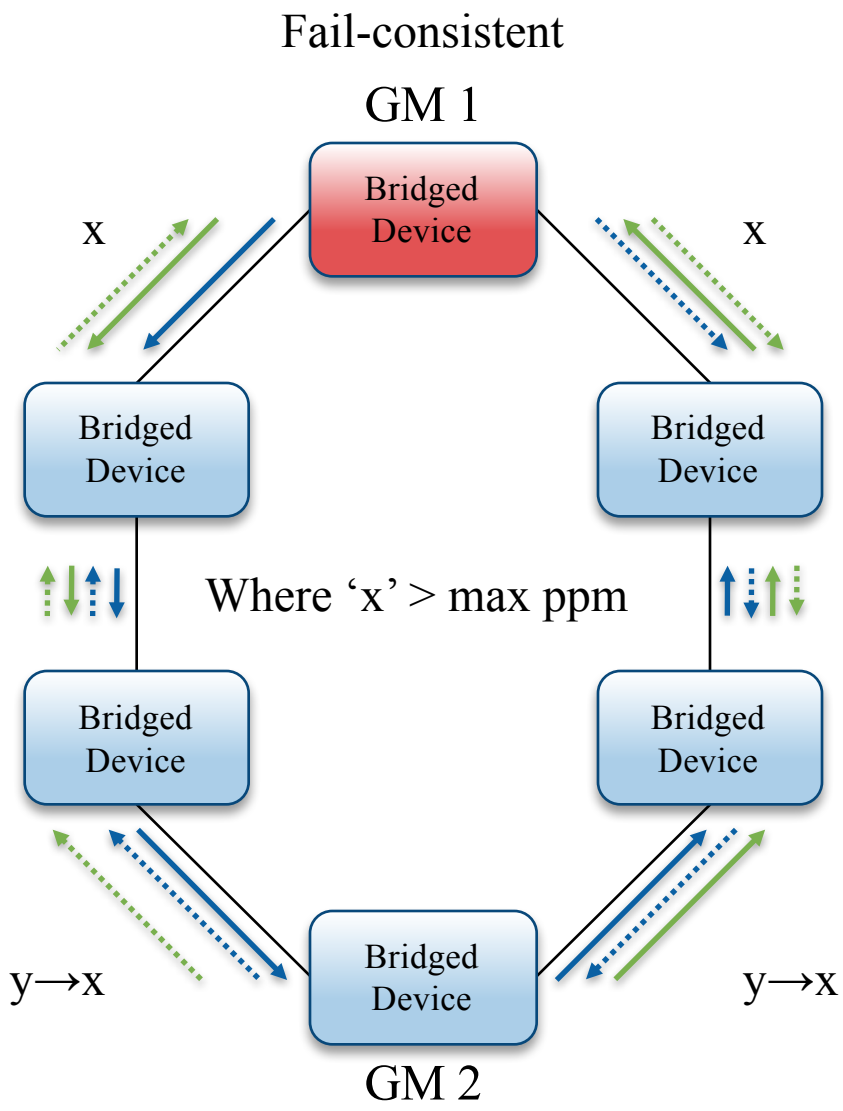
Redundancy with 2 GM's

- Observations:
  - Requires 4 domains
    - Seamless path failure requires at least 2 domains per GM (multipath)
  - Requires convergence of time between GM's
    - Prevents phase shift during faults
- Advantages:
  - Addresses engineered networks
  - Addresses seamless path failures
  - Addresses seamless 'fail-silent'
- Disadvantages:
  - Does not address 'fail-consistent'



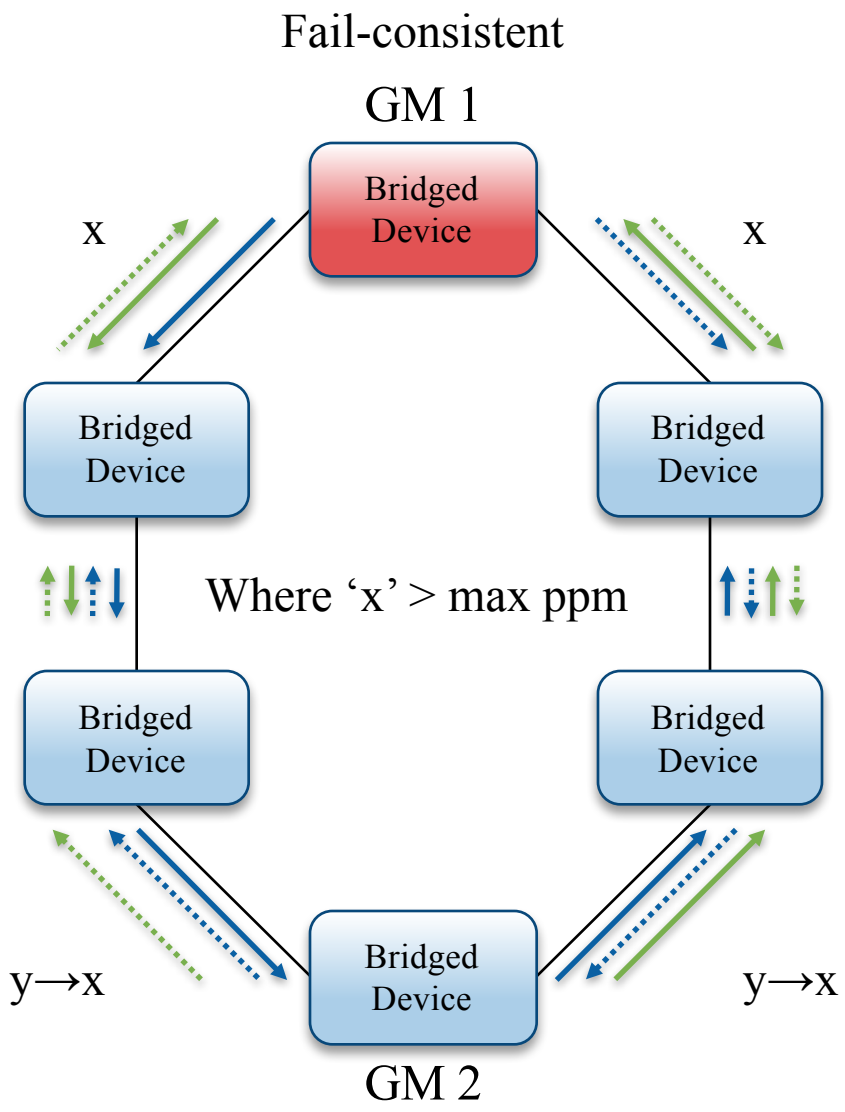
Redundancy with 2 GM's

- Observations:
  - Requires 4 domains
    - Seamless path failure requires at least 2 domains per GM (multipath)
  - Requires convergence of time between GM's
    - Prevents phase shift during faults
- Advantages:
  - Addresses engineered networks
  - Addresses seamless path failures
  - Addresses seamless 'fail-silent'
- Disadvantages:
  - Does not address 'fail-consistent'



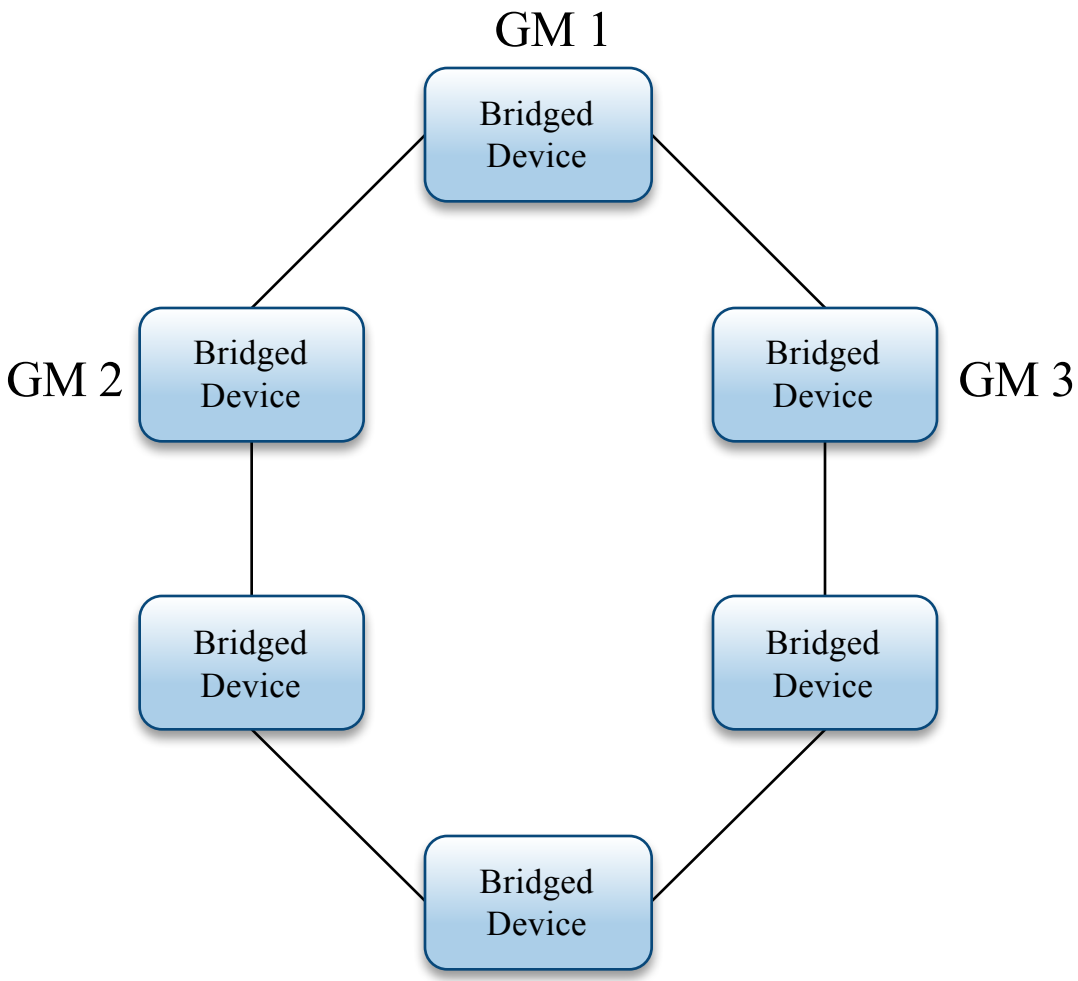
Redundancy with 2 GM's

- Observations:
  - Requires 4 domains
    - Seamless path failure requires at least 2 domains per GM (multipath)
  - Requires convergence of time between GM's
    - Prevents phase shift during faults
- Advantages:
  - Addresses engineered networks
  - Addresses seamless path failures
  - Addresses seamless 'fail-silent'
- Disadvantages:
  - Does not address 'fail-consistent'
  - Does not address 'fail-inconsistent (byzantine)'



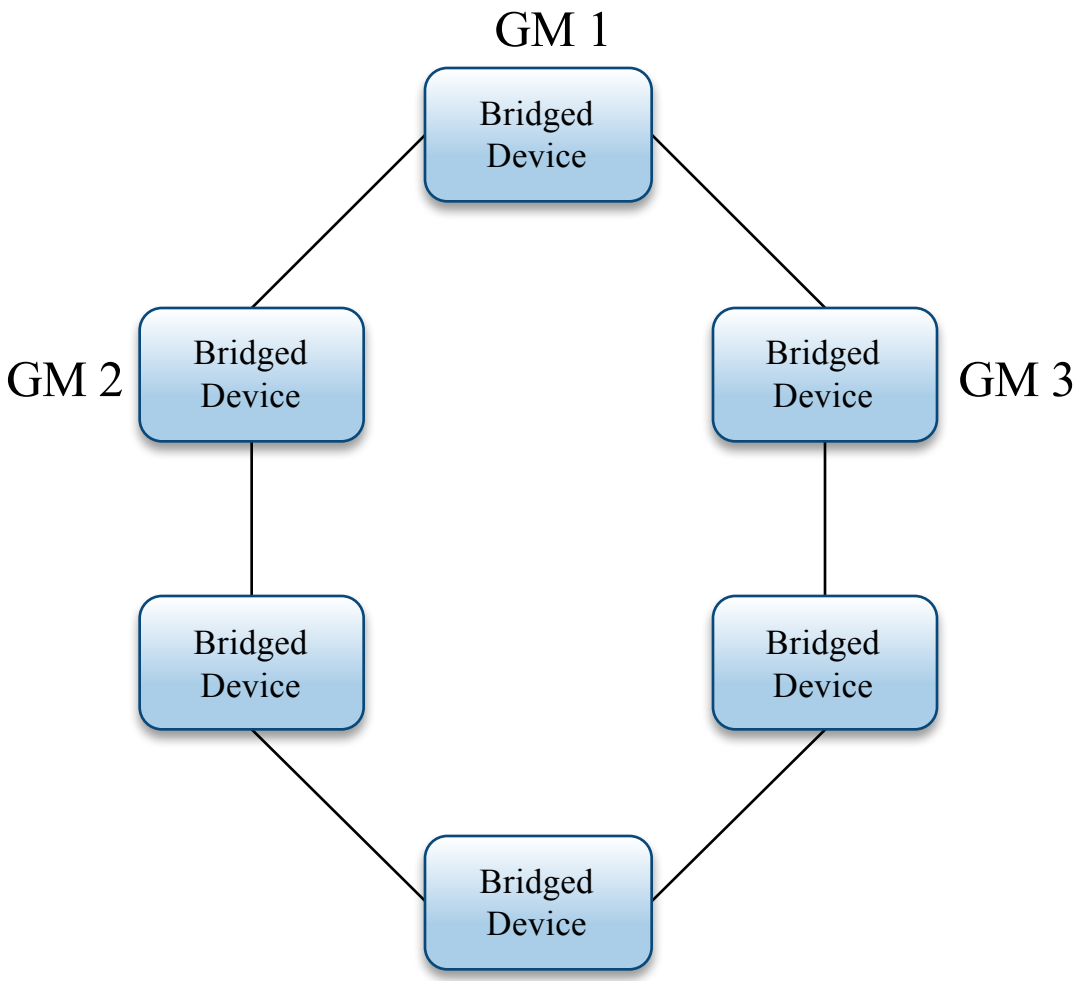
Redundancy with 3 GM's

- Observations:
  - Requires 6 domains
    - Seamless path failure requires at least 2 domains per GM (multipath)
  - Requires convergence of time between GM's
    - Prevents phase shift during faults



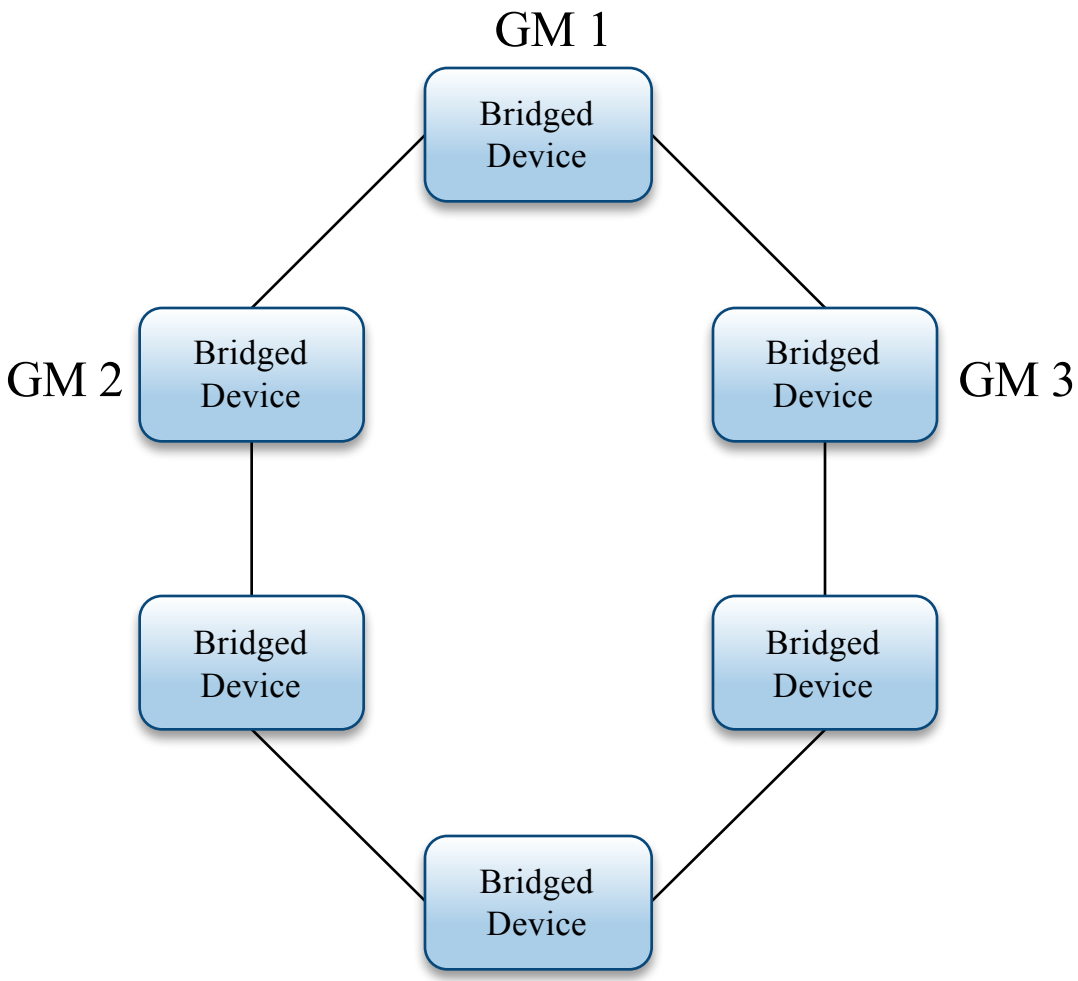
Redundancy with 3 GM's

- Observations:
  - Requires 6 domains
    - Seamless path failure requires at least 2 domains per GM (multipath)
  - Requires convergence of time between GM's
    - Prevents phase shift during faults
  - Slaves need to know
    - When majority of GMs are converged (> ½)
    - Which GM(s) to ignore



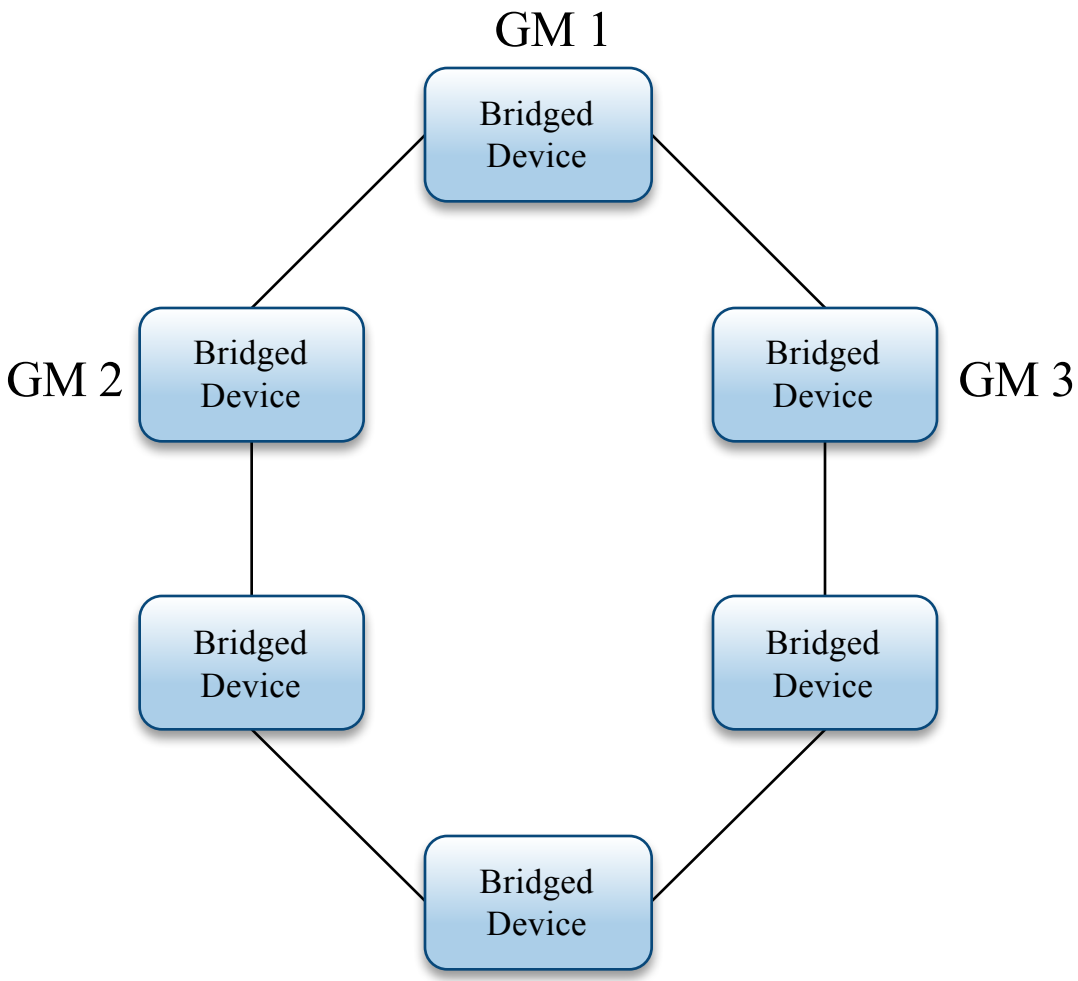
Redundancy with 3 GM's

- Observations:
  - Requires 6 domains
    - Seamless path failure requires at least 2 domains per GM (multipath)
  - Requires convergence of time between GM's
    - Prevents phase shift during faults
  - Slaves need to know
    - When majority of GMs are converged (> ½)
    - Which GM(s) to ignore
- Advantages:
  - Addresses engineered networks
  - Addresses seamless path failures
  - Addresses seamless 'fail-silent'
  - Addresses seamless 'fail-consistent'



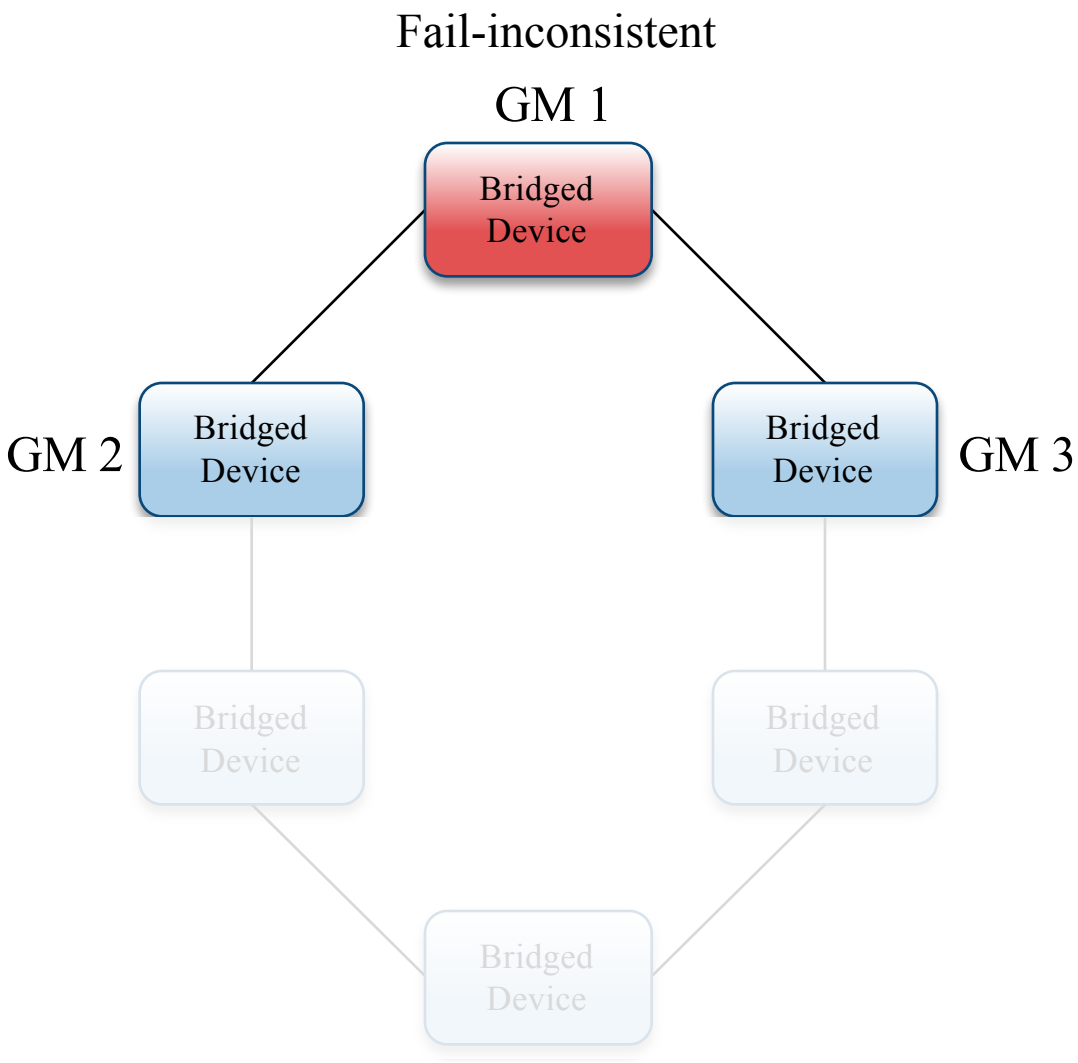
Redundancy with 3 GM's

- Observations:
  - Requires 6 domains
    - Seamless path failure requires at least 2 domains per GM (multipath)
  - Requires convergence of time between GM's
    - Prevents phase shift during faults
  - Slaves need to know
    - When majority of GMs are converged (> ½)
    - Which GM(s) to ignore
- Advantages:
  - Addresses engineered networks
  - Addresses seamless path failures
  - Addresses seamless 'fail-silent'
  - Addresses seamless 'fail-consistent'
- Disadvantages:
  - Does not address 'fail-inconsistent (byzantine)'



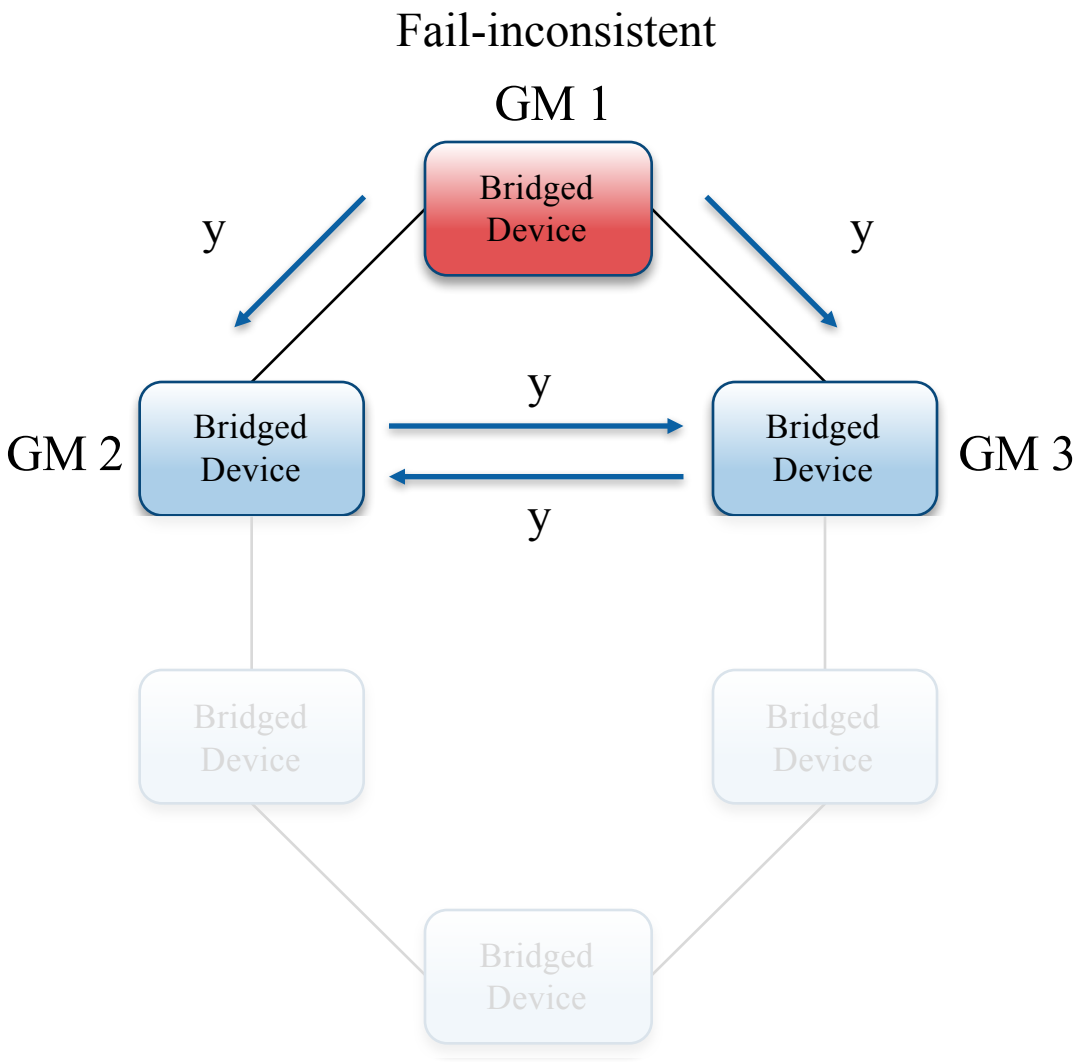
Redundancy with 3 GM's

- Observations:
  - Requires 6 domains
    - Seamless path failure requires at least 2 domains per GM (multipath)
  - Requires convergence of time between GM's
    - Prevents phase shift during faults
  - Slaves need to know
    - When majority of GMs are converged (> ½)
    - Which GM(s) to ignore
- Advantages:
  - Addresses engineered networks
  - Addresses seamless path failures
  - Addresses seamless 'fail-silent'
  - Addresses seamless 'fail-consistent'
- Disadvantages:
  - Does not address 'fail-inconsistent (byzantine)'



Redundancy with 3 GM's

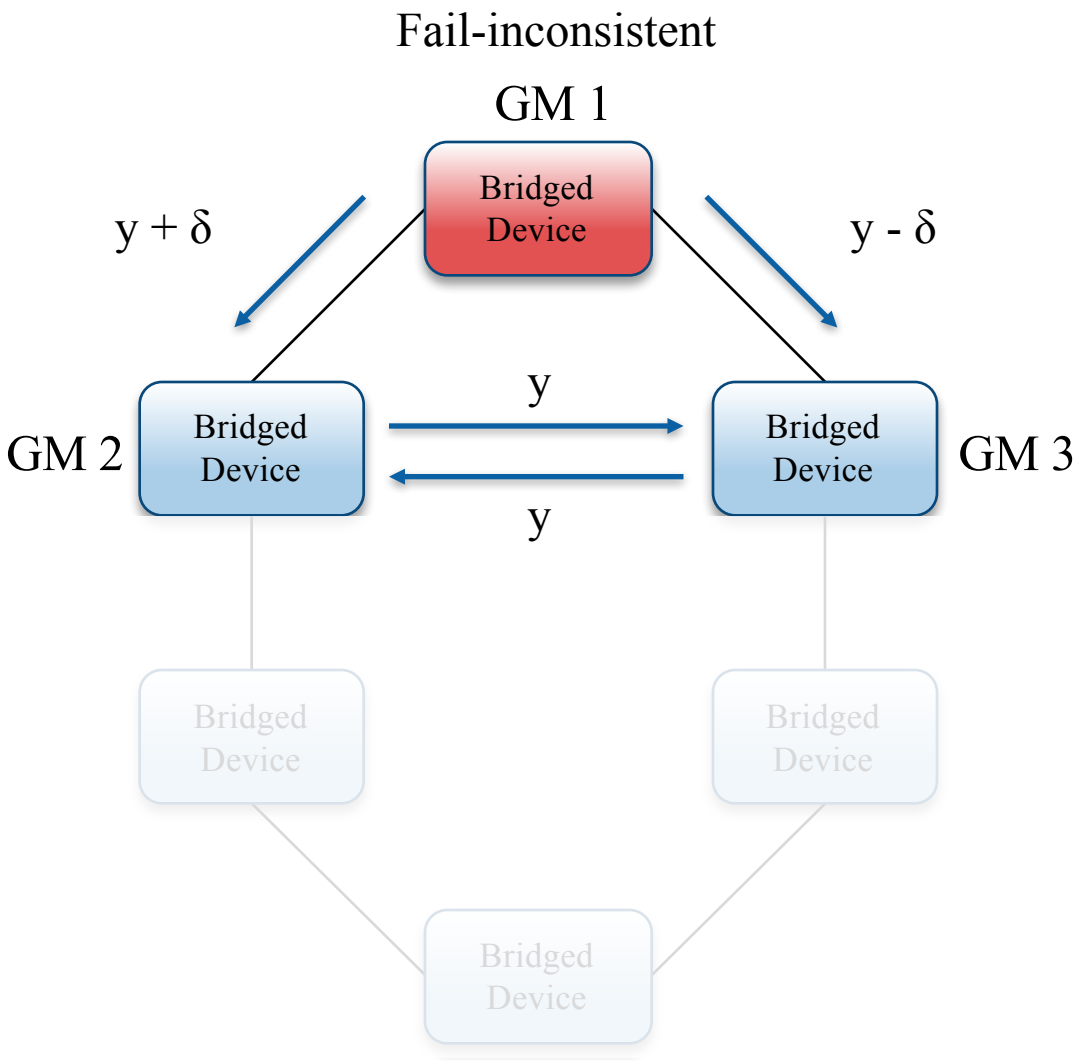
- Observations:
  - Requires 6 domains
    - Seamless path failure requires at least 2 domains per GM (multipath)
  - Requires convergence of time between GM's
    - Prevents phase shift during faults
  - Slaves need to know
    - When majority of GMs are converged (> ½)
    - Which GM(s) to ignore
- Advantages:
  - Addresses engineered networks
  - Addresses seamless path failures
  - Addresses seamless 'fail-silent'
  - Addresses seamless 'fail-consistent'
- Disadvantages:
  - Does not address 'fail-inconsistent (byzantine)'



NATIONAL INSTRUMENTS

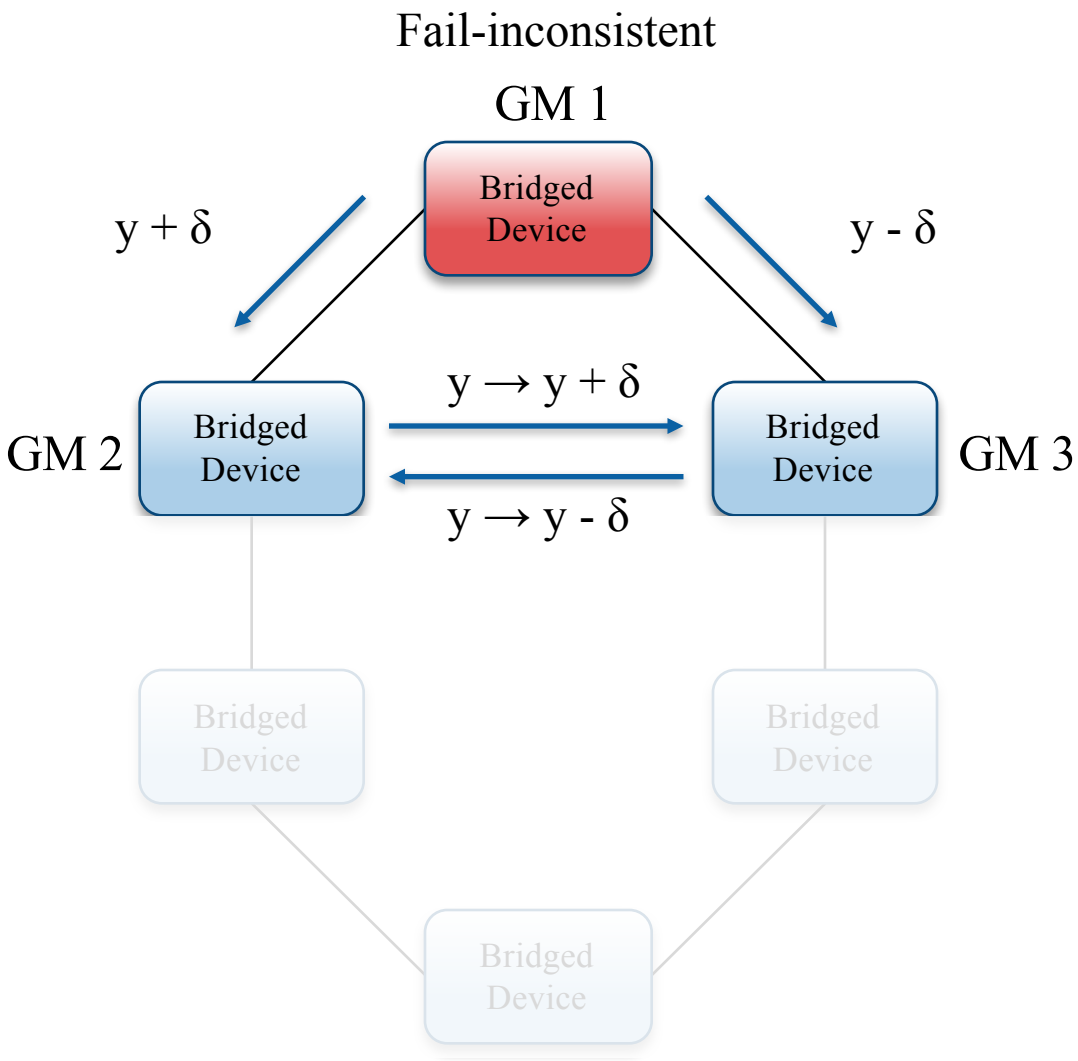
Redundancy with 3 GM's

- Observations:
  - Requires 6 domains
    - Seamless path failure requires at least 2 domains per GM (multipath)
  - Requires convergence of time between GM's
    - Prevents phase shift during faults
  - Slaves need to know
    - When majority of GMs are converged (> ½)
    - Which GM(s) to ignore
- Advantages:
  - Addresses engineered networks
  - Addresses seamless path failures
  - Addresses seamless 'fail-silent'
  - Addresses seamless 'fail-consistent'
- Disadvantages:
  - Does not address 'fail-inconsistent (byzantine)'



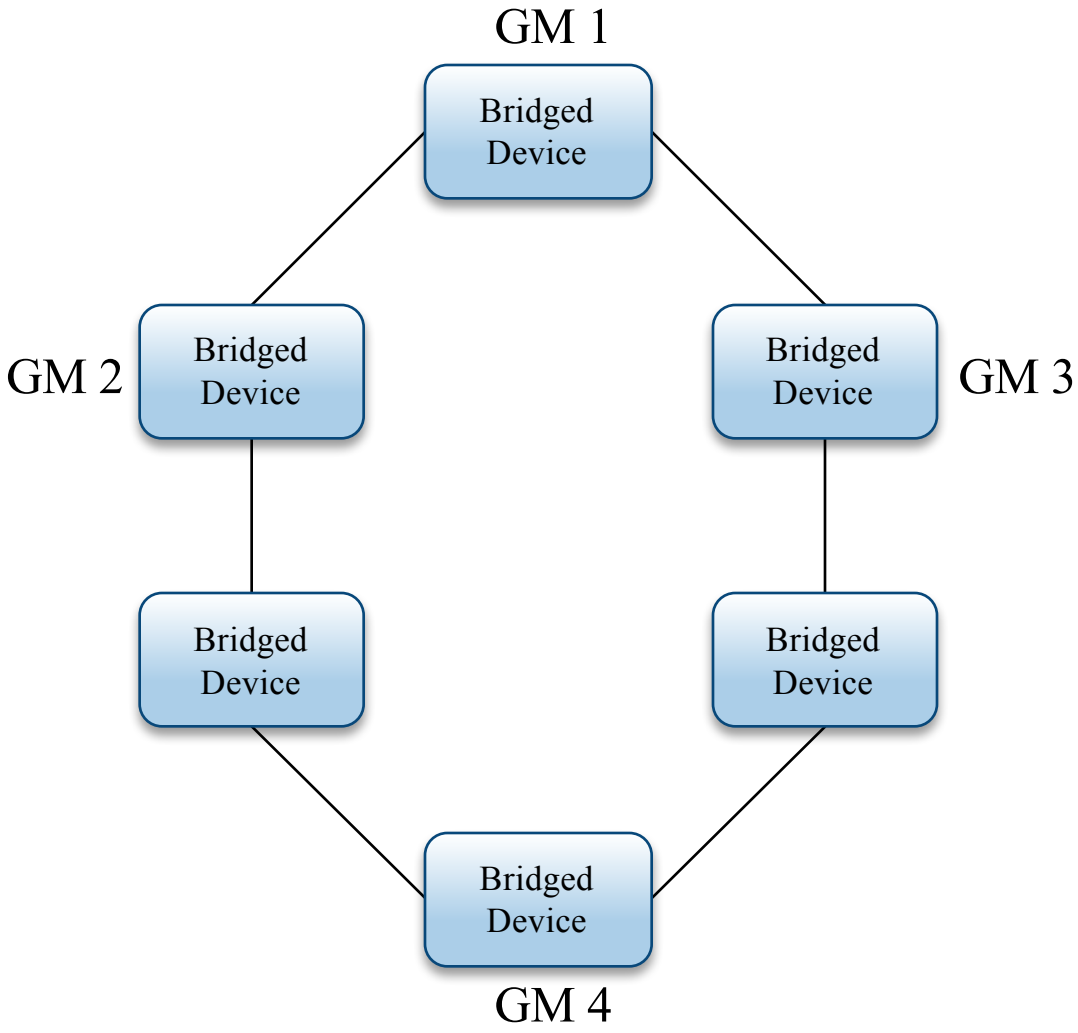
Redundancy with 3 GM's

- Observations:
  - Requires 6 domains
    - Seamless path failure requires at least 2 domains per GM (multipath)
  - Requires convergence of time between GM's
    - Prevents phase shift during faults
  - Slaves need to know
    - When majority of GMs are converged (> ½)
    - Which GM(s) to ignore
- Advantages:
  - Addresses engineered networks
  - Addresses seamless path failures
  - Addresses seamless 'fail-silent'
  - Addresses seamless 'fail-consistent'
- Disadvantages:
  - Does not address 'fail-inconsistent (byzantine)'



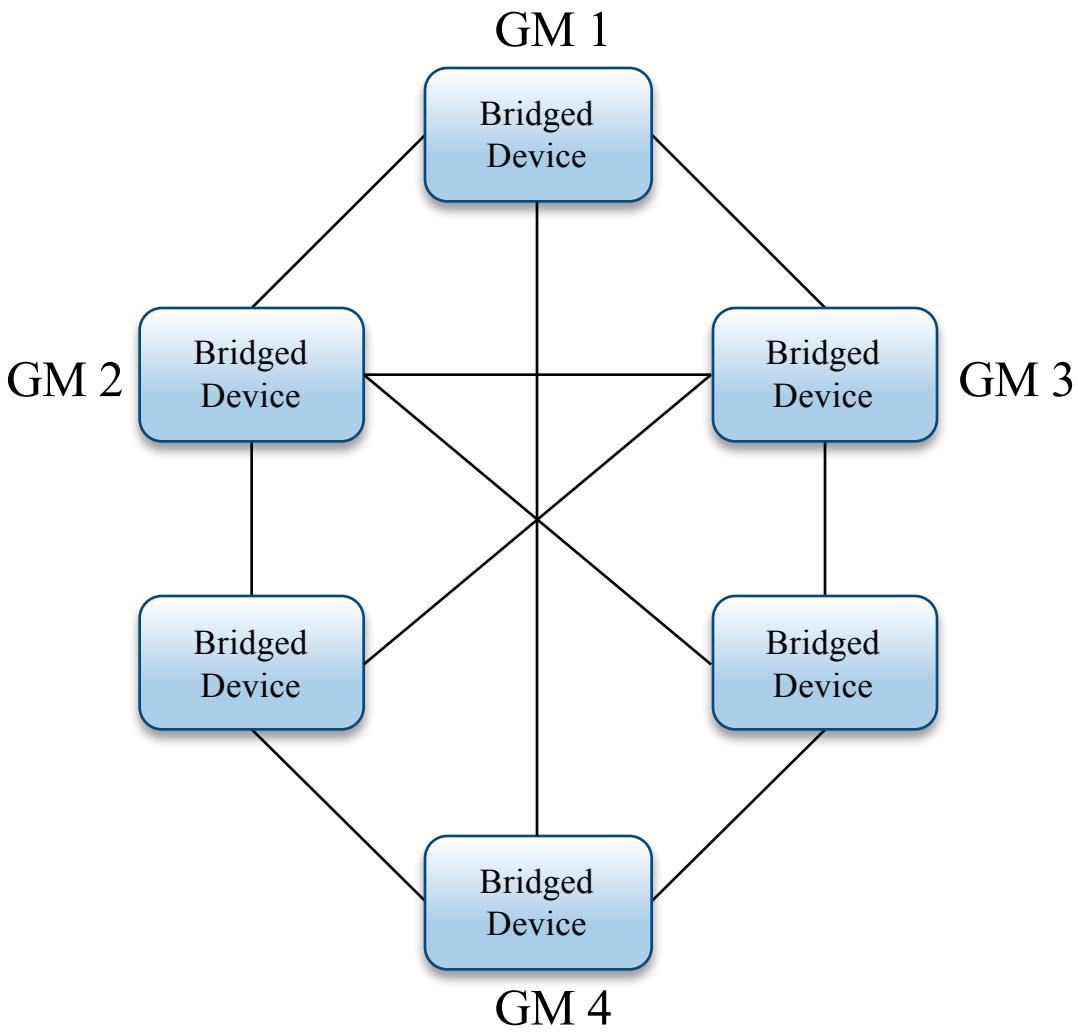
Redundancy with 4 GM's

- Observations:
  - Requires 8 domains
    - Seamless path failure requires at least 2 domains per GM (multipath)
  - Requires convergence of time between GM's
    - Prevents phase shift during faults
  - Slaves need to know
    - majority of GMs are converged (> 2/3)
    - Which GM(s) to ignore



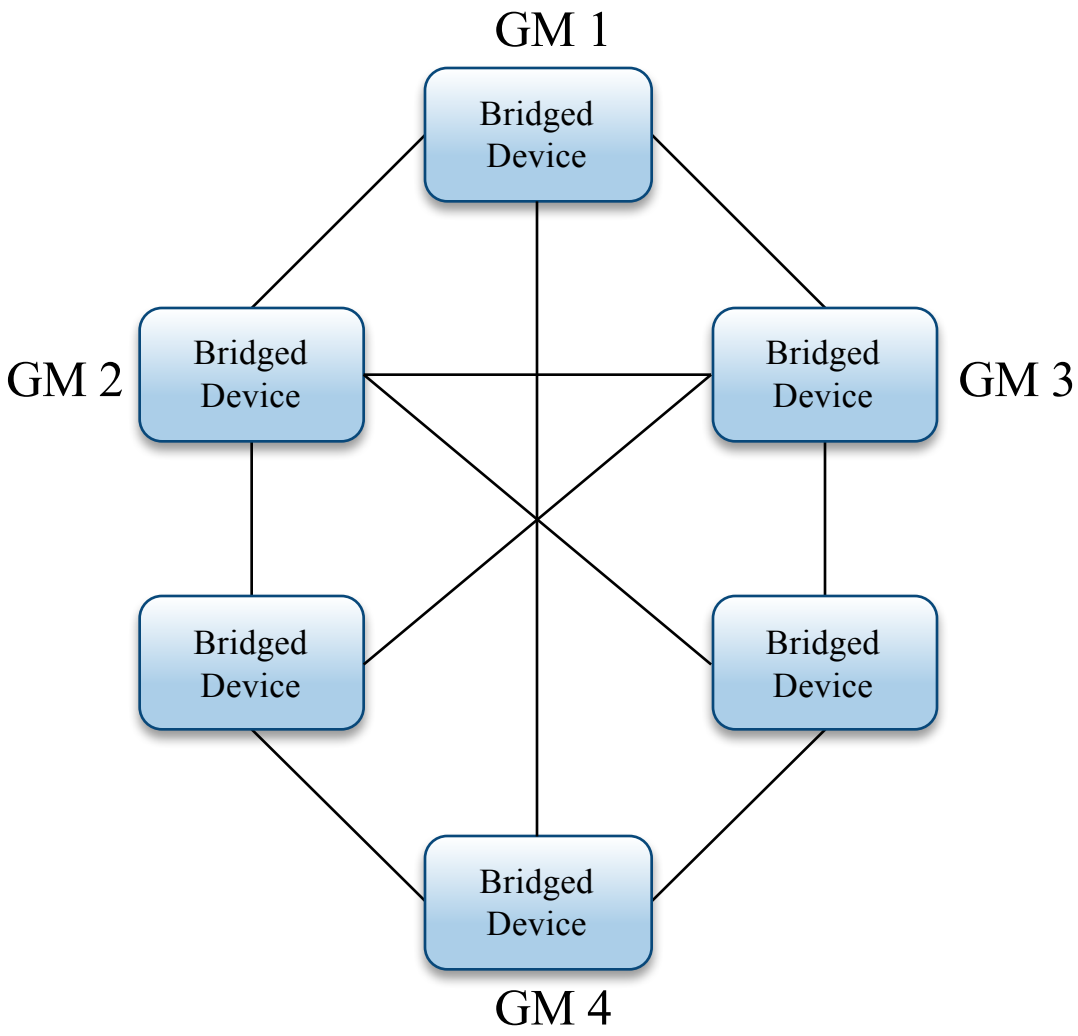
Redundancy with 4 GM's

- Observations:
  - Requires 8 domains
    - Seamless path failure requires at least 2 domains per GM (multipath)
  - Requires convergence of time between GM's
    - Prevents phase shift during faults
  - Slaves need to know
    - majority of GMs are converged (> 2/3)
    - Which GM(s) to ignore
  - Requires 3 disjoint paths to GM's



Redundancy with 4 GM's

- Observations:
  - Requires 8 domains
    - Seamless path failure requires at least 2 domains per GM (multipath)
  - Requires convergence of time between GM's
    - Prevents phase shift during faults
  - Slaves need to know
    - majority of GMs are converged (> 2/3)
    - Which GM(s) to ignore
  - Requires 3 disjoint paths to GM's
- Advantages:
  - Addresses engineered networks
  - Addresses seamless path failures
  - Addresses seamless 'fail-silent'
  - Addresses seamless 'fail-consistent'
  - Addresses seamless 'fail-inconsistent (byzantine)'



NATIONAL INSTRUMENTS

Proposed Assumptions

- One solution that is scalable
  - Fail-silent to fail-inconsistent
  - One device failure to N device failures

- .1AS redundancy can specify a single algorithm as the default.
  - Cover a wide variety of applications