Perfect Failure Detector
Interface of Perfect Failure Detector

- **Module:**
  - Name: PerfectFailureDetector, instance $P$

- **Events:**
  - **Indication:** $\langle P, \text{Crash} \mid p_i \rangle$
    - Notifies that node $p_i$ has crashed

- **Properties:**
  - $PFD1$ (*strong completeness*)
  - $PFD2$ (*strong accuracy*)
Properties of P

Properties:

- **PFD1 (strong completeness)**
  - Eventually every node that **crashes** is permanently detected by every correct node (**liveness**)

- **PFD2 (strong accuracy)**
  - If a node p is detected by any node, then p has crashed (**safety**)

Safety or Liveness?
Implementing P in Synchrony

- **Assume** synchronous system
  - Max transmission delay between 0 and $\delta$ time units

- Each node every $\gamma$ time units
  - Send <heartbeat> to all nodes

- Each node waits $\gamma+\delta$ time units
  - If did not get <heartbeat> from $p_i$
    - Detect <crash | $p_i$>
Correctness of P

- **PFD1 (strong completeness)**
  - A crashed node doesn’t send <heartbeat>
  - Eventually every node will notice the absence of <heartbeat>
Correctness of P

**PFD2 (strong accuracy)**

- Assuming local computation is negligible
- Maximum time between 2 heartbeats
  - $\gamma + \delta$ time units
- If alive, all nodes will recv hb in time
  - No inaccuracy

![Diagram](image-url)