Agenda Item 3: SWIM Architecture

David Leow

6 May 2024

CAAS
Civil Aviation Authority of Singapore

Introduction

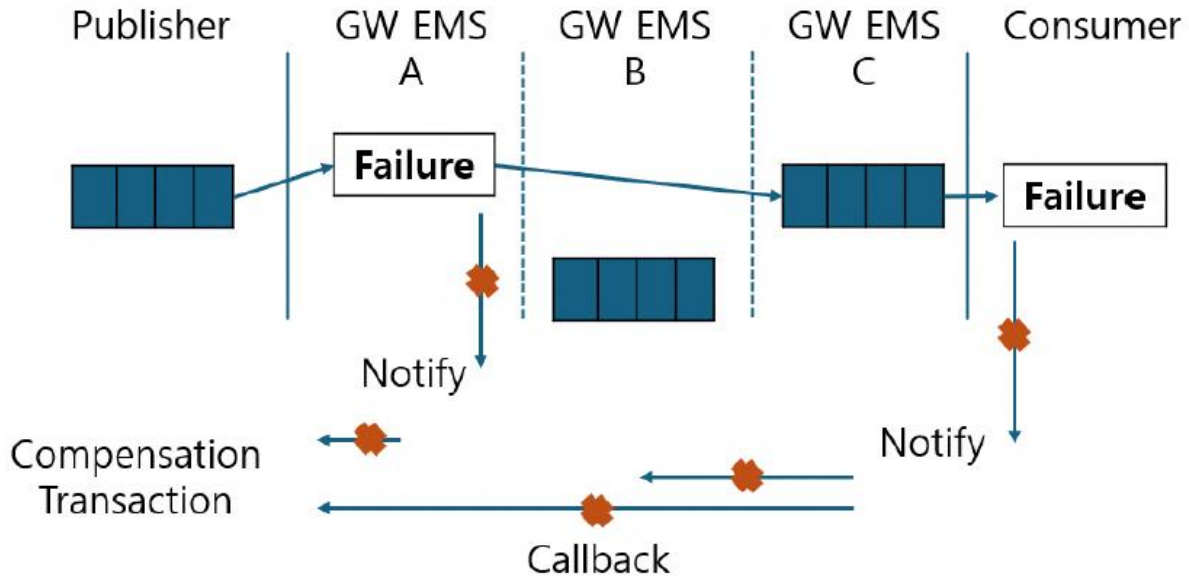
- Needed a more detailed architecture that conforms with the agreed distributed architecture to support the demonstration and trial.
- 2 options – both options will conform to the agreed distributed SWIM architecture
  - Hierarchical Model
  - Mesh Model
- SWIM TF chose to use the Hierarchical Model to support the SWIM over CRV demo and Surveillance Sharing over SWIM ops trial.
- Several lessons learnt from using this model post event.

Extracts from SWIM TF/9-WP/10(1)

1. Prioritizing of messages is not possible
   - Congestion on the network will prevent message prioritization.
   - Assuming the use of the single message queue per subscriber
2. Guaranteed message delivery failure due to improper failover or message handling during partitioning phase
   - Artifact of the implementation of APAC SWIM. Not everyone using the same type of EMS
   - guaranteed message delivery mechanism implementation all different and incompatible.
   - Destroyed when message broker malfunctions.
     - Once the message broker reaches its maximum number of messages, it will start dropping messages.
     - Breaks the guaranteed message delivery mechanism.

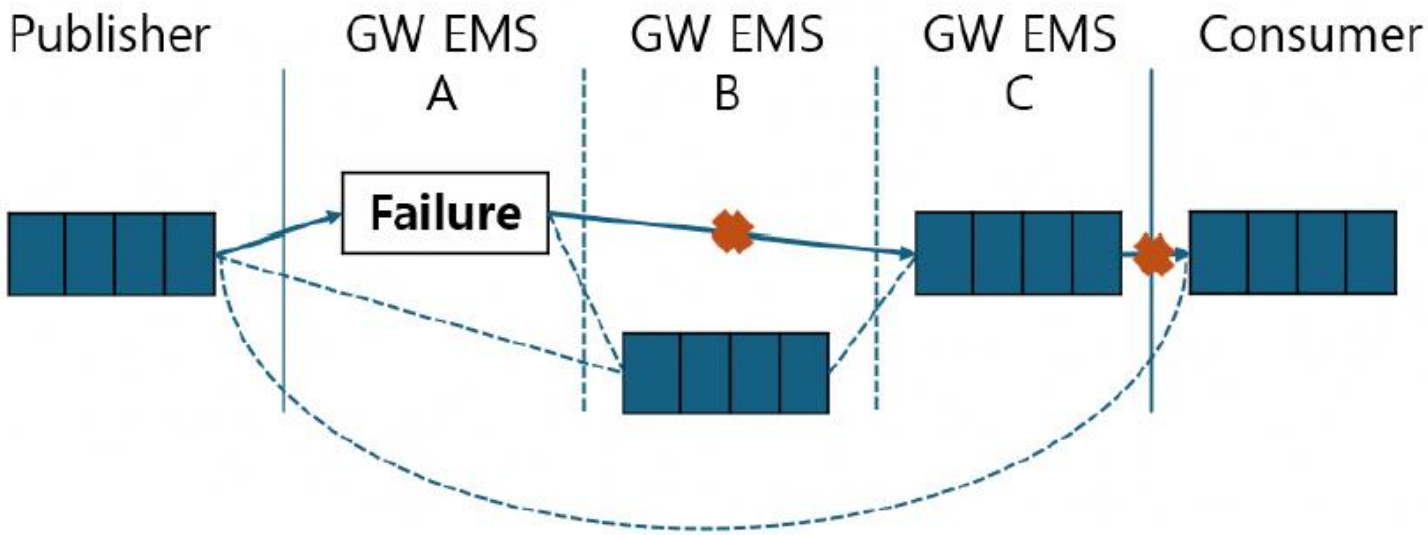
Extracts from SWIM TF/9-WP/10(2)

3. Compensation transaction cannot be performed
   - Publisher can only be aware of transmission failure at the immediate neighbouring EMS, e.g. edge to gateway.
   - Beyond the immediate neighbours no way to tell if there has been a transmission failure
   - So cannot resend to compensate.



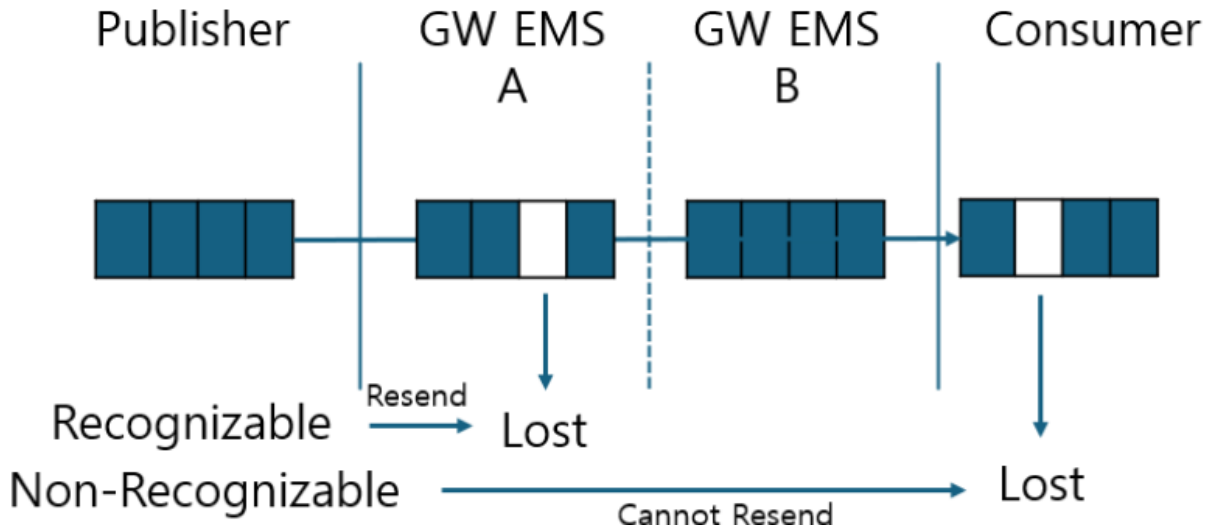
Extracts from SWIM TF/9-WP/10(3)

4. Not able to use detour route in the event of a message delivery failure.
   - Architecture not setup with redundant/alternate routes
   - CRV supports any-to-any connection but we restrict it with the hierarchy architecture.
   - Publisher not able to resend the message even if it recognizes a failure in delivery



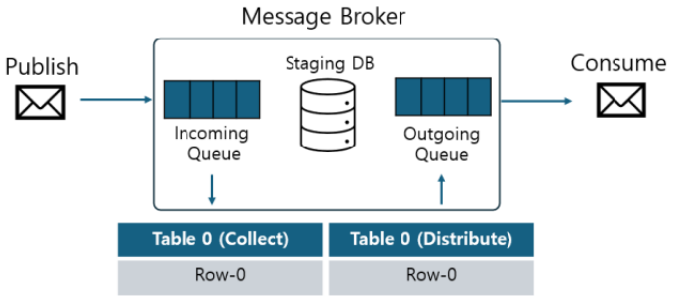
Extracts from SWIM TF/9-WP/10(4)

5. Edge node does not know which message to resend when message loss occurs
   - The publisher is able to determine the missing message in a broker directly connected to it.
   - However, if the message loss occurs further downstream, there is no way for the publisher to know which message to resend.



Proposed solutions

- WP/10 proposed some solutions for each of the 5 problem statements
  - Issue 1: Priority Messaging
    - Using message brokers to set message priorities.
    - Higher priority messages are consumed before messages with lower priorities
  - Issue 2: Guaranteed Messging
    - Leaky Bucket Algorithm
    - Use of a JMS Server with staging DB
  - Issue 3: Compensation Transactions
    - Use Saga pattern to maintain data cons
  - Issue 4: Alternate Path
    - Open Shortest Path First
  - Issue 5: Resending of lost message
    - Automatic Repeat reQuest (ARQ)
    - Consumer to acknowledge to producer upon message receipt.



Arguments for Mesh Architecture

- Some solutions rely on OSI Layer 3 implementation.
  - May not be practical to implement
- Switching to a mesh architecture will immediately resolve issues 3 and 4
  - Mesh architecture means that there will be no intermediate gateway EMS. All EMS are connected.
    - Issue 3 will no longer exists as the consumer will be able to notify the producer of a delivery failure.
    - Issue 4 will also no longer exists as it will become like issue 3.
- However, issues 1, 2 and 5 will still need to be addressed.
- There may be other issues with Mesh Architecture that we are not aware of.
  - Do another trial with the same scenarios as the joint event but on mesh architecture
  - To help discover the vulnerabilities.

Arguments against Mesh Architecture

- Queue management
- GRE Tunnel Setup – PCCW push back.
  - Update from CRV OG – PCCW is willing to support limited mesh connections between the Gateway EMSs
- Need to trial to find out more deficiencies.

Further considerations for Hierarchical Architecture.

- If we choose hierarchical architecture there are some further considerations that we need to consider
  - How messages are to be routed (To be further discussed in Agenda item 5)
  - Limits on the number of Gateway EMS to exists in the APAC SWIM
  - Requirements on Gateway EMS providers.
- Number of Gateway EMS
  - There should only be a limited number of Gateways.
    - Not every ANSP can or should become a gateway EMS
  - Maximum of 8 should be more than sufficient
- Requirements on Gateway EMS providers
  - To ensure that Gateway EMSs all perform similarly and are interoperable.

Suggested Requirements for Gateway EMS providers

- That the Gateway EMS should be a separate EMS from the provider's own operational EMS
  - Segregation of data flows for better data governance
  - Easier administration
  - Easier maintenance
    - Expect that the Gateway EMS once setup will be quite static as compared to the operational EMS
- Recent demonstrations show that there are some issues communicating between different type of Gateway EMS.
  - Need to find a way to enable easier implementation for intercommunication.

Set Target for implementation for APAC SWIM

- Target initial implementation for APAC SWIM
  - Lead States / Special Administrative Regions
    - Thailand, Singapore, Japan, Korea, China, Hong Kong China,
  - Stretch states
    - Australia, Malaysia, Indonesia, New Zealand, Vietnam