MODULE *IdemProxy*

IdemProxy
- Every request must be hit the server exactly once
- For each request, the response must be the same
- 2 tries / requests must be processable in parallel

EXTENDS *Integers* , *FiniteSets*

CONSTANTS
  $\_ReqIDs$, the request *IDs* sent by the user (an *Id* is the idempotent key)
  $\_MaxTries$,
  $NULL$

ASSUME $\_MaxTries < 10$

VARIABLES
  $tries$, the different tries of specific $\_Requests$
  $hits$, the number of hits of the "protected" backend per requests
  $responses$ the responses received by the client for each try

$vars \triangleq \langle tries, hits, responses \rangle$

Initial State

$Init \triangleq$
  $\land\ tries = [r \in \_ReqIDs \mapsto 0]$
  $\land\ hits = [r\ \in \_ReqIDs \mapsto 0]$
  $\land\ responses = [r \in \_ReqIDs \mapsto NULL]$

$TypeInvariants \triangleq$
  $\land$ TRUE

Actions

$Submit(r) \triangleq$
  $\land\ tries[r] < \_MaxTries$
  $\land\ tries' = [tries$ EXCEPT $![r] = tries[r] + 1]$
  $\land$ UNCHANGED $\langle hits, responses \rangle$

Spec

$Next \triangleq$
  $\lor\ \exists\, r \in \_ReqIDs :$
    $\lor\ Submit(r)$

$Spec \triangleq$
  $\land\ Init$
  $\land\ \Box[Next]_{vars}$