MODULE *Configuration*

INSTANCE *Naturals*

INSTANCE *FiniteSets*

LOCAL INSTANCE *TLC*

An empty constant
CONSTANT *Nil*

Status constants
CONSTANTS
InProgress,
Complete,
Failed

The set of all nodes
CONSTANT *Node*

Target is the set of all targets and their possible paths and values.

Example:
Target $\triangleq$
[*target*1 $\mapsto$
[*persistent* $\mapsto$ FALSE, *values* $\mapsto$ [
*path*1 $\mapsto$ {"*value*1", "*value*2"},
*path*2 $\mapsto$ {"*value*2", "*value*3"}]],
*target*2 $\mapsto$
[*persistent* $\mapsto$ TRUE, *values* $\mapsto$ [
*path*2 $\mapsto$ {"*value*3", "*value*4"},
*path*3 $\mapsto$ {"*value*4", "*value*5"}]]]
CONSTANT *Target*

A record of per-target configurations
VARIABLE *configuration*

A record of target states
VARIABLE *target*

A record of target *masterships*
VARIABLE *mastership*

LOCAL *InitState* $\triangleq$
[*configurations* $\mapsto$ *configuration*,
targets $\mapsto$ *target*,
masterships $\mapsto$ *mastership*]

```
LOCAL NextState ≜
  [configurations ↦ configuration′,
   targets        ↦ target′,
   masterships    ↦ mastership′]

LOCAL Trace ≜ INSTANCE Trace WITH
  Module    ← "Configuration",
  InitState ← InitState,
  NextState ← NextState
```

This section models the *Configuration* reconciler.

```
Reconcile(n, t) ≜
  ∧ ∨ ∧ Target[t].persistent
      ∧ configuration[t].state ≠ Complete
      ∧ configuration′ = [configuration EXCEPT ![t].state = Complete]
      ∧ UNCHANGED ⟨target⟩
    ∨ ∧ ¬Target[t].persistent
      ∧ ∨ mastership[t].term > configuration[t].config.term
        ∨ ∧ mastership[t].term = configuration[t].config.term
          ∧ mastership[t].master = Nil
      ∧ configuration′ = [configuration EXCEPT ![t].config.term = mastership[t].term,
                                               ![t].state       = InProgress]
      ∧ UNCHANGED ⟨target⟩
    ∨ ∧ configuration[t].state = InProgress
      ∧ mastership[t].term = configuration[t].config.term
      ∧ mastership[t].master = n
      ∧ target′ = [target EXCEPT ![t] = configuration[t].target.values]
      ∧ configuration′ = [configuration EXCEPT ![t].target.term = mastership[t].term,
                                               ![t].state       = Complete]
  ∧ UNCHANGED ⟨mastership⟩
```

Formal specification, constraints, and theorems.

```
Init ≜
  ∧ configuration = [t ∈ DOMAIN Target ↦
                       [state  ↦ InProgress,
                        config ↦
                          [index  ↦ 0,
                           term   ↦ 0,
                           values ↦
                             [path ∈ {} ↦
                                [path  ↦ path,
                                 value ↦ Nil,
```

$$
\begin{array}{l}
\qquad\qquad\qquad\qquad index \mapsto 0,\\
\qquad\qquad\qquad\qquad deleted \mapsto \text{FALSE}]]],\\
\qquad\qquad\qquad proposal \mapsto [index \mapsto 0],\\
\qquad\qquad\qquad commit \mapsto [index \mapsto 0],\\
\qquad\qquad\qquad target \mapsto\\
\qquad\qquad\qquad\quad [index \mapsto 0,\\
\qquad\qquad\qquad\quad\ term \mapsto 0,\\
\qquad\qquad\qquad\quad\ values \mapsto\\
\qquad\qquad\qquad\qquad [path \in \{\} \mapsto\\
\qquad\qquad\qquad\qquad\quad [path \mapsto path,\\
\qquad\qquad\qquad\qquad\quad\ value \mapsto Nil,\\
\qquad\qquad\qquad\qquad\quad\ index \mapsto 0,\\
\qquad\qquad\qquad\qquad\quad\ deleted \mapsto \text{FALSE}]]]]]\\
\quad \land\ Trace!Init
\end{array}
$$

$$
\begin{array}{l}
Next \triangleq\\
\quad \lor\ \exists\, n \in Node :\\
\qquad \exists\, t \in \text{DOMAIN}\ configuration :\\
\qquad\quad Trace!Step(\text{“Reconcile”},\ Reconcile(n,\ t),\ [node \mapsto n,\ target \mapsto t])
\end{array}
$$

* Modification History
* Last modified Sun *Feb* 20 08:17:49 *PST* 2022 by *jordanhalterman*
* Created Sun *Feb* 20 02:21:04 *PST* 2022 by *jordanhalterman*