MODULE *Mastership*

INSTANCE *Naturals*

INSTANCE *FiniteSets*

INSTANCE *Sequences*

An empty constant
CONSTANT *Nil*

The set of possible master nodes
CONSTANT *Node*

Variables defined by other modules.
VARIABLES
conn

A record of target masterships
VARIABLE *mastership*

$$
\begin{array}{l}
TypeOK \triangleq \\
\quad \land\ mastership.term \in Nat \\
\quad \land\ mastership.master \neq Nil \Rightarrow mastership.master \in Node \\
\quad \land\ mastership.conn \in Nat
\end{array}
$$

$$
\begin{array}{l}
Test \triangleq \text{INSTANCE } Test \text{ WITH} \\
\quad File \leftarrow \text{“Mastership.log”}, \\
\quad CurrState \leftarrow [\\
\qquad mastership \mapsto mastership, \\
\qquad conn \mapsto conn], \\
\quad SuccState \leftarrow [\\
\qquad mastership \mapsto mastership', \\
\qquad conn \mapsto conn']
\end{array}
$$

This section models *mastership* for the configuration service.

Mastership is used primarily to track the lifecycle of individual configuration targets and react to state changes on the southbound. Each target is assigned a master from the *Node* set, and masters can be unset when the target disconnects.

$$
\begin{array}{l}
ReconcileMastership(n) \triangleq \\
\quad \land\ \lor\ \land\ conn[n].connected \\
\qquad\quad \land\ mastership.master = Nil \\
\qquad\quad \land\ mastership' = [
\end{array}
$$

$$
\begin{array}{l}
\qquad\qquad\quad master \mapsto n, \\
\qquad\qquad\quad term \quad\ \mapsto mastership.term + 1, \\
\qquad\qquad\quad conn \quad\ \mapsto conn[n].id] \\
\quad \lor \ \land \ \lor \neg conn[n].connected \\
\qquad\quad\ \ \lor conn[n].id \neq mastership.conn \\
\qquad\ \ \land mastership.master = n \\
\qquad\ \ \land mastership' = [mastership \ \text{EXCEPT} \ !.master = Nil] \\
\land \ \text{UNCHANGED} \ \langle conn \rangle
\end{array}
$$