MODULE *Device*

EXTENDS *Naturals*, *FiniteSets*, *Sequences*, *Messages*

Device states
CONSTANTS *Running*, *Stopped*

The following variables are used by the device to track *mastership*.

The current state of the device, either *Running* or *Stopped*
VARIABLE *state*

A mapping of stream election *IDs*
VARIABLE *election*

The following variables are used for model checking.

A history of successful writes to the switch used for model checking
VARIABLE *history*

Device related variables
$deviceVars \triangleq \langle state, election, history \rangle$

Device state related variables
$stateVars \triangleq \langle state \rangle$

This section models a *P4* Runtime device. For the purposes of this spec, the device has two functions: determine a master controller node and accept writes. Mastership is determined through *MasterArbitrationUpdates* sent by the controller nodes. The 'election_id's provided by controller nodes are stored in 'elections', and the master is computed as the node with the highest 'election_id' at any given time. The device will only allow writes from the current master node.

Returns the set of election *IDs* in the given elections
$ElectionIds(e) \triangleq \{e[x] : x \in \text{DOMAIN } e\}$

Returns the maximum value from a set or undefined if the set is empty
$Max(s) \triangleq \text{CHOOSE } x \in s : \forall\, y \in s : x \geq y$

Returns the highest election *ID* for the given elections
$MaxElectionId(e) \triangleq Max(ElectionIds(e))$

Returns the master for the given elections
$MasterId(e) \triangleq$
    IF $Cardinality(\{i \in ElectionIds(e) : i > 0\}) > 0$ THEN
        CHOOSE $n \in$ DOMAIN $e : e[n] = MaxElectionId(e)$

ELSE
Nil

Shuts down the device

When the device is shutdown, all the volatile device and stream variables are set back to their initial state. The 'writeTerm' accepted by the device is persisted through the restart.

$$
\begin{aligned}
&\mathit{Shutdown} \triangleq \\
&\quad \land\ \mathit{state} = \mathit{Running} \\
&\quad \land\ \mathit{state}' = \mathit{Stopped} \\
&\quad \land\ \mathit{responseStream}' = [n \in \text{DOMAIN } \mathit{responseStream} \mapsto [\mathit{id} \mapsto \mathit{responseStream}[n].\mathit{id},\ \mathit{state} \mapsto \mathit{Closed}]] \\
&\quad \land\ \mathit{requests}' = [n \in \text{DOMAIN } \mathit{requests} \mapsto \langle\rangle] \\
&\quad \land\ \mathit{responses}' = [n \in \text{DOMAIN } \mathit{responses} \mapsto \langle\rangle] \\
&\quad \land\ \mathit{election}' = [n \in \text{DOMAIN } \mathit{election} \mapsto 0] \\
&\quad \land\ \text{UNCHANGED } \langle \mathit{requestStream},\ \mathit{history} \rangle
\end{aligned}
$$

Starts the device

$$
\begin{aligned}
&\mathit{Startup} \triangleq \\
&\quad \land\ \mathit{state} = \mathit{Stopped} \\
&\quad \land\ \mathit{state}' = \mathit{Running} \\
&\quad \land\ \text{UNCHANGED } \langle \mathit{messageVars},\ \mathit{election},\ \mathit{history},\ \mathit{streamVars} \rangle
\end{aligned}
$$

Connects a new stream between node 'n' and the device

When a stream is connected, the 'streams' state for node 'n' is set to *Open*. Stream creation is modelled as a single step to reduce the state space.

$$
\begin{aligned}
&\mathit{ConnectStream}(n) \triangleq \\
&\quad \land\ \mathit{state} = \mathit{Running} \\
&\quad \land\ \mathit{requestStream}[n].\mathit{state} = \mathit{Open} \\
&\quad \land\ \mathit{responseStream}[n].\mathit{id} < \mathit{requestStream}[n].\mathit{id} \\
&\quad \land\ \mathit{responseStream}[n].\mathit{state} = \mathit{Closed} \\
&\quad \land\ \mathit{responseStream}' = [\mathit{responseStream} \text{ EXCEPT } ![n].\mathit{state} = \mathit{Open}] \\
&\quad \land\ \text{UNCHANGED } \langle \mathit{deviceVars},\ \mathit{messageVars},\ \mathit{requestStream} \rangle
\end{aligned}
$$

Disconnects an open stream between node 'n' and the device

When a stream is disconnected, the 'streams' state for node 'n' is set to *Closed*, any 'election_id' provided by node 'n' is forgotten, and the 'requests' and 'responses' queues for the node are cleared. Additionally, if the stream belonged to the master node, a new master is elected and a *MasterArbitrationUpdate* is sent on the streams that remain in the *Open* state. The *MasterArbitrationUpdate* will be sent to the new master with a 'status' of *Ok* and to all slaves with a 'status' of *AlreadyExists*.

$$
\begin{aligned}
&\mathit{DisconnectStream}(n) \triangleq \\
&\quad \land\ \mathit{state} = \mathit{Running} \\
&\quad \land\ \mathit{responseStream}[n].\mathit{state} = \mathit{Open} \\
&\quad \land\ \mathit{election}' = [\mathit{election} \text{ EXCEPT } ![n] = 0] \\
&\quad \land\ \mathit{responseStream}' = [\mathit{responseStream} \text{ EXCEPT } ![n].\mathit{state} = \mathit{Closed}] \\
&\quad \land\ \mathit{requests}' = [\mathit{requests} \text{ EXCEPT } ![n] = \langle\rangle] \\
&\quad \land\ \text{LET } \mathit{oldMaster} \triangleq \mathit{MasterId}(\mathit{election}) \\
&\qquad\quad \mathit{newMaster} \triangleq \mathit{MasterId}(\mathit{election}')
\end{aligned}
$$

```
    IN
        ∨ ∧ oldMaster ≠ newMaster
          ∧ responses' = [i ∈ DOMAIN responseStream' ↦
                            IF responseStream'[i].state = Open THEN
                                IF i = newMaster THEN
                                    Append(responses[i], [
                                        type        ↦ MasterArbitrationUpdate,
                                        status      ↦ Ok,
                                        election_id ↦ MaxElectionId(election')])
                                ELSE
                                    Append(responses[i], [
                                        type        ↦ MasterArbitrationUpdate,
                                        status      ↦ AlreadyExists,
                                        election_id ↦ MaxElectionId(election')])
                            ELSE
                                ⟨⟩]
        ∨ ∧ oldMaster = newMaster
          ∧ responses' = [responses EXCEPT ![n] = ⟨⟩]
    ∧ UNCHANGED ⟨stateVars, requestStream, history⟩
```

The device receives and responds to a *MasterArbitrationUpdate* from node 'n'

If the 'election_id' is already present in the 'elections' and does not already belong to node 'n', the stream is *Closed* and 'requests' and 'responses' are cleared for the node. If the 'election_id' is not known to the device, it's added to the 'elections' state. If the change results in a new master being elected by the device, a *MasterArbitrationUpdate* is sent on all *Open* streams. If the change does not result in a new master being elected by the device, node 'n' is returned a *MasterArbitrationUpdate*. The device master will always receive a *MasterArbitrationUpdate* response with 'status' of *Ok*, and slaves will always receive a 'status' of *AlreadyExists*.

```
HandleMasterArbitrationUpdate(n) ≜
    ∧ state = Running
    ∧ responseStream[n].state = Open
    ∧ HasRequest(n, MasterArbitrationUpdate)
    ∧ LET r ≜ NextRequest(n)
      IN
        ∨ ∧ r.election_id ∈ ElectionIds(election)
          ∧ election[n] ≠ r.election_id
          ∧ responseStream' = [responseStream EXCEPT ![n].state = Closed]
          ∧ requests' = [requests EXCEPT ![n] = ⟨⟩]
          ∧ responses' = [responses EXCEPT ![n] = ⟨⟩]
          ∧ UNCHANGED ⟨deviceVars⟩
        ∨ ∧ r.election_id ∉ ElectionIds(election)
          ∧ election' = [election EXCEPT ![n] = r.election_id]
          ∧ LET oldMaster ≜ MasterId(election)
                newMaster ≜ MasterId(election')
            IN
```

```
        ∨ ∧ oldMaster ≠ newMaster
          ∧ responses' = [i ∈ DOMAIN responseStream ↦
                            IF responseStream[i].state = Open THEN
                              IF i = newMaster THEN
                                Append(responses[i], [
                                  type        ↦ MasterArbitrationUpdate,
                                  status      ↦ Ok,
                                  election_id ↦ MaxElectionId(election')])
                               ELSE
                                Append(responses[i], [
                                  type        ↦ MasterArbitrationUpdate,
                                  status      ↦ AlreadyExists,
                                  election_id ↦ MaxElectionId(election')])
                             ELSE
                               responses[i]]
        ∨ ∧ oldMaster = newMaster
          ∧ ∨ ∧ n = newMaster
              ∧ SendResponse(n, [
                  type        ↦ MasterArbitrationUpdate,
                  status      ↦ Ok,
                  election_id ↦ MaxElectionId(election')])
            ∨ ∧ n ≠ newMaster
              ∧ SendResponse(n, [
                  type        ↦ MasterArbitrationUpdate,
                  status      ↦ AlreadyExists,
                  election_id ↦ MaxElectionId(election')])
          ∧ UNCHANGED ⟨responseStream⟩
    ∧ DiscardRequest(n)
    ∧ UNCHANGED ⟨stateVars, requestStream, history⟩
```

The device receives a *WriteRequest* from node 'n'

The *WriteRequest* is accepted if:
* The 'election_id' for node 'n' matches the 'election_id' for its stream
* Node 'n' is the current master for the device
* If a 'token' is provided in the *WroteRequest* and the 'token' is greater than or equal to the last 'writeToken' accepted by the device

When the *WriteRequest* is accepted, the 'writeToken' is updated and the term of the node that sent the request is recorded for model checking. If the *WriteRequest* is rejeceted, a *PermissionDenied* response is returned.

```
HandleWrite(n) ≜
    ∧ state = Running
    ∧ responseStream[n].state = Open
    ∧ HasRequest(n, WriteRequest)
    ∧ LET r ≜ NextRequest(n)
      IN
          ∨ ∧ election[n] = r.election_id
```

$$
\begin{array}{l}
\quad \land \mathit{MasterId}(\mathit{election}) = n \\
\quad \land \mathit{history}' = \mathit{Append}(\mathit{history}, [\mathit{node} \mapsto n, \mathit{term} \mapsto r.\mathit{term}]) \\
\quad \land \mathit{SendResponse}(n, [\\
\qquad \mathit{type} \quad \mapsto \mathit{WriteResponse}, \\
\qquad \mathit{status} \mapsto \mathit{Ok}]) \\
\lor \land \lor \mathit{election}[n] \neq r.\mathit{election\_id} \\
\quad \lor \mathit{MasterId}(\mathit{election}) \neq n \\
\quad \land \mathit{SendResponse}(n, [\\
\qquad \mathit{type} \quad \mapsto \mathit{WriteResponse}, \\
\qquad \mathit{status} \mapsto \mathit{PermissionDenied}]) \\
\quad \land \text{UNCHANGED } \langle \mathit{history} \rangle \\
\land \mathit{DiscardRequest}(n) \\
\land \text{UNCHANGED } \langle \mathit{stateVars}, \mathit{election}, \mathit{streamVars} \rangle
\end{array}
$$

* Modification History
* Last modified *Wed Mar* 27 13:08:01 *PDT* 2019 by *jordanhalterman*
* Created *Wed Feb* 20 23:49:17 *PST* 2019 by *jordanhalterman*