
MODULE *Device*

EXTENDS *Naturals, FiniteSets, Sequences, Messages*

Device states

CONSTANTS *Running, Stopped*

The current state of the device

VARIABLE *state*

The election *ID* for each node

VARIABLE *election*

The current epoch for each node

VARIABLE *epoch*

The epoch of the last successful write to the device

VARIABLE *maxEpoch*

Device state change count used for enforcing state constraints

VARIABLE *stateChanges*

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

VARIABLE *history*

Device related variables

$deviceVars \triangleq \langle state, election, epoch, maxEpoch, history, stateChanges \rangle$

Device state related variables

$stateVars \triangleq \langle state, stateChanges \rangle$

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 'maxEpoch' accepted by the device is persisted through the restart.

```

Shutdown  $\triangleq$ 
   $\wedge state = Running$ 
   $\wedge state' = Stopped$ 
   $\wedge responseStream' = [n \in DOMAIN responseStream \mapsto [id \mapsto responseStream[n].id, state \mapsto Closed]]$ 
   $\wedge requests' = [n \in DOMAIN requests \mapsto \langle \rangle]$ 
   $\wedge responses' = [n \in DOMAIN responses \mapsto \langle \rangle]$ 
   $\wedge election' = [n \in DOMAIN election \mapsto 0]$ 
   $\wedge epoch' = [n \in DOMAIN epoch \mapsto 0]$ 
   $\wedge stateChanges' = stateChanges + 1$ 
   $\wedge UNCHANGED \langle maxEpoch, requestStream, history \rangle$ 

```

Starts the device

```

Startup  $\triangleq$ 
   $\wedge state = Stopped$ 
   $\wedge state' = Running$ 
   $\wedge stateChanges' = stateChanges + 1$ 
   $\wedge UNCHANGED \langle messageVars, election, epoch, maxEpoch, history, streamVars \rangle$ 

```

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

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

```

ConnectStream(n)  $\triangleq$ 
   $\wedge state = Running$ 
   $\wedge requestStream[n].state = Open$ 
   $\wedge responseStream[n].id < requestStream[n].id$ 
   $\wedge responseStream[n].state = Closed$ 
   $\wedge responseStream' = [responseStream \text{ EXCEPT } ![n].state = Open]$ 
   $\wedge UNCHANGED \langle deviceVars, messageVars, requestStream \rangle$ 

```

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

When a stream is closed, 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*.

```

DisconnectStream(n)  $\triangleq$ 
   $\wedge state = Running$ 
   $\wedge responseStream[n].state = Open$ 

```

$$\begin{aligned}
& \wedge \text{election}' = [\text{election} \text{ EXCEPT } ![n] = 0] \\
& \wedge \text{epoch}' = [\text{epoch} \text{ EXCEPT } ![n] = 0] \\
& \wedge \text{responseStream}' = [\text{responseStream} \text{ EXCEPT } ![n].\text{state} = \text{Closed}] \\
& \wedge \text{requests}' = [\text{requests} \text{ EXCEPT } ![n] = \langle \rangle] \\
& \wedge \text{LET } \text{oldMaster} \triangleq \text{MasterId}(\text{election}) \\
& \quad \text{newMaster} \triangleq \text{MasterId}(\text{election}') \\
& \text{IN} \\
& \quad \vee \wedge \text{oldMaster} \neq \text{newMaster} \\
& \quad \quad \wedge \text{responses}' = [i \in \text{DOMAIN } \text{responseStream}' \mapsto \\
& \quad \quad \quad \text{IF } \text{responseStream}'[i].\text{state} = \text{Open} \text{ THEN} \\
& \quad \quad \quad \quad \text{IF } i = \text{newMaster} \text{ THEN} \\
& \quad \quad \quad \quad \quad \text{Append}(\text{responses}[i], [\\
& \quad \quad \quad \quad \quad \quad \text{type} \quad \quad \mapsto \text{MasterArbitrationUpdate}, \\
& \quad \quad \quad \quad \quad \quad \text{status} \quad \mapsto \text{Ok}, \\
& \quad \quad \quad \quad \quad \quad \text{election_id} \mapsto \text{MaxElectionId}(\text{election}')] \\
& \quad \quad \quad \quad \text{ELSE} \\
& \quad \quad \quad \quad \quad \text{Append}(\text{responses}[i], [\\
& \quad \quad \quad \quad \quad \quad \text{type} \quad \quad \mapsto \text{MasterArbitrationUpdate}, \\
& \quad \quad \quad \quad \quad \quad \text{status} \quad \mapsto \text{AlreadyExists}, \\
& \quad \quad \quad \quad \quad \quad \text{election_id} \mapsto \text{MaxElectionId}(\text{election}')] \\
& \quad \quad \quad \quad \text{ELSE} \\
& \quad \quad \quad \quad \quad \langle \rangle] \\
& \quad \quad \vee \wedge \text{oldMaster} = \text{newMaster} \\
& \quad \quad \quad \wedge \text{responses}' = [\text{responses} \text{ EXCEPT } ![n] = \langle \rangle] \\
& \wedge \text{UNCHANGED } \langle \text{stateVars}, \text{maxEpoch}, \text{requestStream}, \text{history} \rangle
\end{aligned}$$

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*.

$$\begin{aligned}
& \text{HandleMasterArbitrationUpdate}(n) \triangleq \\
& \quad \wedge \text{state} = \text{Running} \\
& \quad \wedge \text{responseStream}[n].\text{state} = \text{Open} \\
& \quad \wedge \text{HasRequest}(n, \text{MasterArbitrationUpdate}) \\
& \quad \wedge \text{LET } r \triangleq \text{NextRequest}(n) \\
& \quad \text{IN} \\
& \quad \quad \vee \wedge r.\text{election_id} \in \text{ElectionIds}(\text{election}) \\
& \quad \quad \quad \wedge \text{election}[n] \neq r.\text{election_id} \\
& \quad \quad \quad \wedge \text{responseStream}' = [\text{responseStream} \text{ EXCEPT } ![n].\text{state} = \text{Closed}] \\
& \quad \quad \quad \wedge \text{requests}' = [\text{requests} \text{ EXCEPT } ![n] = \langle \rangle] \\
& \quad \quad \quad \wedge \text{responses}' = [\text{responses} \text{ EXCEPT } ![n] = \langle \rangle]
\end{aligned}$$

$$\begin{aligned}
& \wedge \text{UNCHANGED } \langle \text{deviceVars} \rangle \\
& \vee \wedge r.\text{election_id} \notin \text{ElectionIds}(\text{election}) \\
& \wedge \text{election}' = [\text{election} \text{ EXCEPT } ![n] = r.\text{election_id}] \\
& \wedge \text{epoch}' = [\text{epoch} \text{ EXCEPT } ![n] = r.\text{epoch}] \\
& \wedge \text{LET } \text{oldMaster} \triangleq \text{MasterId}(\text{election}) \\
& \quad \text{newMaster} \triangleq \text{MasterId}(\text{election}') \\
& \text{IN} \\
& \quad \vee \wedge \text{oldMaster} \neq \text{newMaster} \\
& \quad \wedge \text{responses}' = [i \in \text{DOMAIN } \text{responseStream} \mapsto \\
& \quad \quad \text{IF } \text{responseStream}[i].\text{state} = \text{Open} \text{ THEN} \\
& \quad \quad \quad \text{IF } i = \text{newMaster} \text{ THEN} \\
& \quad \quad \quad \quad \text{Append}(\text{responses}[i], [\\
& \quad \quad \quad \quad \quad \text{type} \quad \mapsto \text{MasterArbitrationUpdate}, \\
& \quad \quad \quad \quad \quad \text{status} \quad \mapsto \text{Ok}, \\
& \quad \quad \quad \quad \quad \text{election_id} \mapsto \text{MaxElectionId}(\text{election}')] \\
& \quad \quad \quad \text{ELSE} \\
& \quad \quad \quad \quad \text{Append}(\text{responses}[i], [\\
& \quad \quad \quad \quad \quad \text{type} \quad \mapsto \text{MasterArbitrationUpdate}, \\
& \quad \quad \quad \quad \quad \text{status} \quad \mapsto \text{AlreadyExists}, \\
& \quad \quad \quad \quad \quad \text{election_id} \mapsto \text{MaxElectionId}(\text{election}')] \\
& \quad \quad \quad \text{ELSE} \\
& \quad \quad \quad \quad \text{responses}[i]] \\
& \quad \vee \wedge \text{oldMaster} = \text{newMaster} \\
& \quad \wedge \vee \wedge n = \text{newMaster} \\
& \quad \quad \wedge \text{SendResponse}(n, [\\
& \quad \quad \quad \text{type} \quad \mapsto \text{MasterArbitrationUpdate}, \\
& \quad \quad \quad \text{status} \quad \mapsto \text{Ok}, \\
& \quad \quad \quad \text{election_id} \mapsto \text{MaxElectionId}(\text{election}')] \\
& \quad \vee \wedge n \neq \text{newMaster} \\
& \quad \quad \wedge \text{SendResponse}(n, [\\
& \quad \quad \quad \text{type} \quad \mapsto \text{MasterArbitrationUpdate}, \\
& \quad \quad \quad \text{status} \quad \mapsto \text{AlreadyExists}, \\
& \quad \quad \quad \text{election_id} \mapsto \text{MaxElectionId}(\text{election}')] \\
& \quad \wedge \text{UNCHANGED } \langle \text{responseStream} \rangle \\
& \wedge \text{DiscardRequest}(n) \\
& \wedge \text{UNCHANGED } \langle \text{stateVars}, \text{maxEpoch}, \text{requestStream}, \text{history} \rangle
\end{aligned}$$

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 node 'n' provided an 'epoch' and the 'epoch' is greater than or equal to the highest epoch received by the device

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

$$\begin{aligned}
& \text{HandleWrite}(n) \triangleq \\
& \quad \wedge \text{state} = \text{Running} \\
& \quad \wedge \text{responseStream}[n].\text{state} = \text{Open} \\
& \quad \wedge \text{HasRequest}(n, \text{WriteRequest}) \\
& \quad \wedge \text{LET } r \triangleq \text{NextRequest}(n) \\
& \quad \text{IN} \\
& \quad \quad \vee \wedge \text{election}[n] = r.\text{election_id} \\
& \quad \quad \quad \wedge \text{MasterId}(\text{election}) = n \\
& \quad \quad \quad \wedge \text{epoch}[n] > 0 \Rightarrow \text{epoch}[n] \geq \text{maxEpoch} \\
& \quad \quad \quad \wedge \text{maxEpoch}' = \text{epoch}[n] \\
& \quad \quad \quad \wedge \text{history}' = \text{Append}(\text{history}, [\text{node} \mapsto n, \text{term} \mapsto r.\text{term}]) \\
& \quad \quad \quad \wedge \text{SendResponse}(n, [\\
& \quad \quad \quad \quad \text{type} \mapsto \text{WriteResponse}, \\
& \quad \quad \quad \quad \text{status} \mapsto \text{Ok}]) \\
& \quad \quad \vee \wedge \vee \text{election}[n] \neq r.\text{election_id} \\
& \quad \quad \quad \vee \text{MasterId}(\text{election}) \neq n \\
& \quad \quad \quad \vee \wedge \text{epoch}[n] > 0 \\
& \quad \quad \quad \quad \wedge \text{epoch}[n] < \text{maxEpoch} \\
& \quad \quad \quad \wedge \text{SendResponse}(n, [\\
& \quad \quad \quad \quad \text{type} \mapsto \text{WriteResponse}, \\
& \quad \quad \quad \quad \text{status} \mapsto \text{PermissionDenied}]) \\
& \quad \quad \quad \wedge \text{UNCHANGED } \langle \text{maxEpoch}, \text{history} \rangle \\
& \quad \wedge \text{DiscardRequest}(n) \\
& \quad \wedge \text{UNCHANGED } \langle \text{stateVars}, \text{election}, \text{epoch}, \text{streamVars} \rangle
\end{aligned}$$

\ * Modification History
\ * Last modified *Thu Feb 21 15:10:49 PST 2019* by *jordanhalterman*
\ * Created *Wed Feb 20 23:49:17 PST 2019* by *jordanhalterman*