MODULE *WebServer*

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

CONSTANTS *Clients*, *LoginInfo*, *FileId*, *FileData*, *M*, *NoFile*, *Inactive*
CONSTANTS *AuthClient*(_, _), *Reply*(_, _)

ASSUME $M \in Nat \land M > 0$
ASSUME $\forall\, c,\, l \;\; : AuthClient(c,\, l) \in$ BOOLEAN
ASSUME $\forall\, c,\, m : Reply(c,\, m) \in$ BOOLEAN

VARIABLES *buffer*, *connections*, *files*, *auths*, *control*

$vars \triangleq \langle buffer,\, connections,\, files,\, auths \rangle$

$File \triangleq [data : FileData,\, access :$ SUBSET $Clients]$

$Request \triangleq [type : \{\text{“GET”}\},\, fid : FileId] \cup [type : \{\text{“AUTH”}\},\, data : LoginInfo] \cup$
$[type : \{\text{“POST”}\},\, f : File,\, fid : FileId]$

$Msg \triangleq \{\text{“Succesful login”},\, \text{“Invalid Login”},\, \text{“File Not Found”},$
$\text{“Succesful file upload”},\, \text{“File stored”}\}$

$Respond \triangleq MSG \cup File$

$NoFile \triangleq$ CHOOSE $f : f \notin File$

$Inactive \triangleq$ CHOOSE $x : x \notin Request \cup Respond$

$TypeInv \triangleq \land\, connections \subseteq Clients$
$\land\, auths \subseteq Clients$
$\land\, IsFiniteSet(connections)$
$\land\, buffer \in [c \in Clients \mapsto Request \cup Respond \cup \{Inactive\}]$
$\land\, files \in [fid \;\; \in FileId \mapsto File \cup \{NoFile\}]$
$\land\, control \in [c \in Clients \mapsto \{\text{“rdy”},\, \text{“working”},\, \text{“done”}\}]$

$Init \triangleq \land\, buffer = [c \in Clients \mapsto Inactive]$
$\land\, control = [c \in Clients \mapsto \text{“rdy”}]$
$\land\, connections = \{\}$
$\land\, auths = \{\}$
$\land\, files \;\; = [fid \in FileId \mapsto NoFile]$

$Connect(c) \triangleq \land\, Cardinality(connections) < M$
$\land\, control[c] = \text{“rdy”}$
$\land\, connections' = connections \cup \{c\}$
$\land$ UNCHANGED $\langle buffer,\, files,\, auths,\, control \rangle$

$Req(c) \triangleq \land\, c \in connections$
$\land\, \exists\, req \in Request :$

```
                ∧ buffer′ = [buffer EXCEPT ![c] = req]
                ∧ control′ = [control EXCEPT ![c] = "working"]
                ∧ connections′ = connections \ c
            ∧ UNCHANGED ⟨files, auths⟩

DoGet(c) ≜
    LET req = buffer[c]
    IN  ∧ control[c] = "working"
        ∧ req.type = "GET"
        ∧ buffer′ = [buffer EXCEPT ![c] = IF files[req.fid] = NoFile
                                          THEN "File not found"
                                          ELSE IF files[req.fid].access = {}
                                               THEN files[req.fid]
                                               ELSE IF c ∈ auths ∩ files[req.fid].access
                                                    THEN files[req.fid]
                                                    ELSE "Unauthorized access"]
        ∧ control′ = [control EXCEPT ![c] = "done"]
        ∧ UNCHANGED ⟨files, auths, connections >

DoAuth(c) ≜
    LET req = buffer[c]
    IN  ∧ control[c] = "working"
        ∧ req.type = "AUTH"
        ∧ buffer′ = [buffer EXCEPT ![c] = IF AuthClient(c, req.data)
                                          THEN "Succesful login"
                                          ELSE "Invalid login"]
        ∧ auths′ = IF AuthClient(c, req.data)
                   THEN auths ∪ {c}
                   ELSE auths
        ∧ control′ = [control EXCEPT ![c] = "done"]
        ∧ UNCHANGED ⟨files, connections⟩

DoPost(c) ≜
    LET req = buffer[c]
    IN  ∧ control[c] = "working"
        ∧ req.type = "POST"
        ∧ buffer′ = [buffer EXCEPT ![c] = IF files[req.fid] = NoFile
                                          THEN "Succesful upload"
                                          ELSE "File already stored"]
        ∧ files′ = [files EXCEPT ![req.fid] = IF ![req.fid] = NoFile
                                              THEN req.f
                                              ELSE ![req.fid]]
        ∧ control′ = [control EXCEPT ![c] = "done"]
        ∧ UNCHANGED ⟨auths, connections⟩

Rsp(c) ≜  ∧ control[c] = "done"
```

$\land$ *Reply*$(c,\ buffer[c])$
$\land$ $buffer' = [buffer$ EXCEPT $![c] = Inactive]$
$\land$ $control' = [control$ EXCEPT $![c] =$ "rdy"$]$
$\land$ UNCHANGED $\langle files,\ auth,\ connections\rangle$

$Next \triangleq \exists\, c \in Clients : Connect(c) \lor Req(c) \lor DoGet(c)$
$\lor\ DoPost(c) \lor DoAuth(c) \lor Rsp(c)$

$Fairness \triangleq$
$\forall\, c \in Clients : \mathrm{WF}_{vars}(DoGet(c) \lor DoPost(c) \lor DoAuth(c) \lor Rsp(c))$

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

THEOREM $Spec \Rightarrow \Box TypeInv$