```
──────────────── MODULE Broker ────────────────
EXTENDS $MQTTBase$

$HandleConnectReq \triangleq$
        $\land\ Len(network[broker]) > 0$
        $\land$ LET $msg \triangleq Head(network[broker])$ IN
                $\land\ msg.to = broker$
                $\land\ msg.type = CONNECT$
                $\land\ \exists\, m \in msgs :$
                        $\land\ m.type\ = CONACK$
                        $\land\ m.from = msg.to$
                        $\land\ m.to = msg.from$
                        $\land\ network' = response(m,\ m.from,\ m.to)$
                        $\land\ active' = active \cup \{msg.from\}$
        $\land$ UNCHANGED $pc$
        $\land$ UNCHANGED $topic\_subscribers$
        $\land$ UNCHANGED $store$
        $\land$ UNCHANGED $used\_num$

$HandleSubscribeReq \triangleq$
        $\land\ Len(network[broker]) > 0$
        $\land$ LET $msg \triangleq Head(network[broker])$ IN
                $\land\ msg.from \in active$
                $\land\ msg.to = broker$
                $\land\ msg.type = SUBSCRIBE$
                $\land\ \exists\, m \in msgs :$
                        $\land\ m.type\ = SUBACK$
                        $\land\ m.from = msg.to$
                        $\land\ m.to = msg.from$
                        $\land\ m.topic = msg.topic$
                        $\land\ m.qos = msg.qos$
                        $\land$ LET $q \triangleq$ CASE $m.qos = 0 \rightarrow QoS0 \Box m.qos = 1 \rightarrow QoS1 \Box m.qos = 2 \rightarrow QoS2$ IN
                                $\land\ topic\_subscribers' = [topic\_subscribers$ EXCEPT $![m.topic][q] = @ \cup \{msg.fro$
                                $\land\ network' =\ response(m,\ m.from,\ m.to)$
        $\land$ UNCHANGED $\langle pc,\ active \rangle$
        $\land$ UNCHANGED $store$
        $\land$ UNCHANGED $used\_num$

$HandleUnsubscribeReq \triangleq$
        $\land\ Len(network[broker]) > 0$
        $\land$ LET $msg \triangleq Head(network[broker])$ IN
                $\land\ msg.from \in active$
                $\land\ msg.to = broker$
                $\land\ msg.type = UNSUBSCRIBE$
                    $\land\ \exists\, m \in msgs :$
                            $\land\ m.type\ = UNSUBACK$
                        $\land m.from = msg.to$
                        $\land m.to = msg.from$
                        $\land m.topic = msg.topic$
                        $\land canSendTo(m.to)$
                        $\land \exists\, q \in \{QoS0,\ QoS1,\ QoS2\} :$
                            $\land topic\_subscribers[msg.topic][q] \neq \{\}$
                            $\land topic\_subscribers' = [topic\_subscribers$ EXCEPT $![m.topic][q] = @ \setminus \{ms$
                            $\land network' = response(m,\ m.from,\ m.to)$
      $\land$ UNCHANGED $\langle pc,\ active \rangle$
      $\land$ UNCHANGED $store$
      $\land$ UNCHANGED $used\_num$

$HandlePingReq \triangleq$
      $\land Len(network[broker]) > 0$
      $\land$ LET $msg \triangleq Head(network[broker])$IN
            $\land\ msg.from \in active$
            $\land\ msg.to = broker$
            $\land\ msg.type = PINGREQ$
            $\land\ \exists\, m \in msgs :$
                 $\land m.type\ = PINGRESP$
                 $\land m.from = msg.to$
                 $\land m.to = msg.from$
                 $\land network' = response(m,\ m.from,\ m.to)$
      $\land$ UNCHANGED $pc$
   $\land$ UNCHANGED $active$
      $\land$ UNCHANGED $topic\_subscribers$
   $\land$ UNCHANGED $store$
      $\land$ UNCHANGED $used\_num$

$HandlePublishWithQoS0Req \triangleq$
      $\land Len(network[broker]) > 0$
      $\land$ LET $msg \triangleq Head(network[broker])$IN
            $\land\ msg.to = broker$
            $\land\ msg.type = PUBLISH$
            $\land\ msg.qos = 0$
            $\land\ network' = rcv(msg,\ broker)$
            $\land\ store' = [store$ EXCEPT $![broker][msg.topic][QoS0] = Append(@,\ msg.packetID)]$
      $\land$ UNCHANGED $pc$
   $\land$ UNCHANGED $active$
   $\land$ UNCHANGED $topic\_subscribers$
      $\land$ UNCHANGED $used\_num$

$HandlePublishWithQoS1Req \triangleq$
      $\land Len(network[broker]) > 0$
      $\land$ LET $msg \triangleq Head(network[broker])$IN
            $\land\ msg.to = broker$
```

```
              $\land\ msg.type = PUBLISH$
              $\land\ msg.qos = 1$
              $\land\ \exists\, m \in msgs :$
                    $\land\ m.type\ = PUBACK$
                    $\land\ m.from = msg.to$
                    $\land\ m.to = msg.from$
                    $\land\ m.packetID = msg.packetID$
                    $\land\ network' = response(m,\ m.from,\ m.to)$
          $\land\ store' = [store\ \text{EXCEPT}\ ![broker][msg.topic][QoS1] = Append(@,\ msg.packetID)]$
       $\land\ \text{UNCHANGED}\ pc$
    $\land\ \text{UNCHANGED}\ active$
    $\land\ \text{UNCHANGED}\ topic\_subscribers$
       $\land\ \text{UNCHANGED}\ used\_num$

$HandlePushQoS1Res\ \triangleq$
       $\land\ Len(network[broker]) > 0$
       $\land\ \text{LET}\ m\ \triangleq\ Head(network[broker])\text{IN}$
              $\land\ \exists\, t \in topics :$
                   $\land\ \exists\, qos \in \{QoS0,\ QoS1,\ QoS2\} :$
                         $\land\ Len(store[broker][t][qos]) > 0$
                         $\land\ m.to = broker$
                         $\land\ m.type = PUBACK$
                         $\land\ m.packetID = Head(store[broker][t][qos]) + maxPubNum$
                         $\land\ network' = rcv(m,\ broker)$
                         $\land\ store' = \text{CASE}\ \ \forall\, q \in \{QoS0,\ QoS1,\ QoS2\} : topic\_subscribers[t][q] \setminus \{m.from\} =$
       $\land\ \text{UNCHANGED}\ pc$
       $\land\ \text{UNCHANGED}\ active$
       $\land\ \text{UNCHANGED}\ topic\_subscribers$
       $\land\ \text{UNCHANGED}\ used\_num$

$HandlePublishWithQoS2Req\ \triangleq$
    $\land\ Len(network[broker]) > 0$
    $\land\ \text{LET}\ msg\ \triangleq\ Head(network[broker])\text{IN}$
       $\land\ msg.to = broker$
       $\land\ msg.type = PUBLISH$
       $\land\ msg.qos = 2$
       $\land\ \exists\, m \in msgs :$
           $\land\ m.type\ = PUBREC$
           $\land\ m.from = msg.to$
           $\land\ m.to = msg.from$
           $\land\ m.packetID = msg.packetID$
           $\land\ network' = response(m,\ m.from,\ m.to)$
           $\land\ store' = [store\ \text{EXCEPT}\ ![broker][msg.topic][QoS2] = Append(@,\ msg.packetID)]$
    $\land\ \text{UNCHANGED}\ pc$
    $\land\ \text{UNCHANGED}\ active$
    $\land$ UNCHANGED $topic\_subscribers$
    $\land$ UNCHANGED $used\_num$

$HandlePubrelReq \triangleq$
    $\land Len(network[broker]) > 0$
    $\land$ LET $msg \triangleq Head(network[broker])$IN
        $\land \ msg.to = broker$
        $\land \ msg.type = PUBREL$
        $\land \ \exists\, m \in msgs :$
            $\land\, m.type \ = PUBCOMP$
            $\land\, m.from = msg.to$
            $\land\, m.to = msg.from$
            $\land\, m.packetID = msg.packetID$
            $\land\, network' = response(m,\ m.from,\ m.to)$
        $\land$ UNCHANGED $store$
    $\land$ UNCHANGED $pc$
    $\land$ UNCHANGED $active$
    $\land$ UNCHANGED $topic\_subscribers$
    $\land$ UNCHANGED $used\_num$

$HandlePushQoS2Res \triangleq$
        $\land Len(network[broker]) > 0$
        $\land$ LET $m \triangleq Head(network[broker])$IN
                $\land \exists\, t \in topics :$
                    $\land \exists\, qos \in \{QoS2\} :$
                        $\land Len(store[broker][t][qos]) > 0$
                        $\land m.from \in subscribers$
                        $\land m.to = broker$
                        $\land m.type = PUBREC$
                        $\land m.packetID = Head(store[broker][t][qos]) + maxPubNum$
                        $\land \exists\, rmsg \in msgs :$
                            $\land \ rmsg.from = m.to$
                            $\land \ rmsg.to = m.from$
                            $\land \ rmsg.type = PUBREL$
                            $\land \ rmsg.packetID = m.packetID$
                            $\land \ network' = response(rmsg,\ rmsg.from,\ rmsg.to)$
        $\land$ UNCHANGED $store$
        $\land$ UNCHANGED $pc$
        $\land$ UNCHANGED $active$
        $\land$ UNCHANGED $topic\_subscribers$
        $\land$ UNCHANGED $used\_num$

$HandlePubCompRes \triangleq$
        $\land Len(network[broker]) > 0$
        $\land$ LET $m \triangleq Head(network[broker])$IN
                $\land \exists\, t \in topics :$
```

```
                    $\land \exists\, qos \in \{QoS2\} :$
                        $\land\, Len(store[broker][t][qos]) > 0$
                        $\land\, m.to = broker$
                        $\land\, m.type = PUBCOMP$
                        $\land\, m.packetID = Head(store[broker][t][qos]) + maxPubNum$
                        $\land\, network' = rcv(m,\, broker)$
                        $\land\, store' =$ CASE $\forall\, q \in \{QoS0,\, QoS1,\, QoS2\} : topic\_subscribers[t][q] \setminus \{m.from\} =$
          $\land$ UNCHANGED $pc$
          $\land$ UNCHANGED $active$
          $\land$ UNCHANGED $topic\_subscribers$
          $\land$ UNCHANGED $used\_num$

$HandleDisConReq \triangleq$
    $\land\, Len(network[broker]) > 0$
    $\land$ LET $msg \triangleq Head(network[broker])$IN
        $\land\ \ msg.to = broker$
        $\land\ \ msg.type = DISCONNECT$
        $\land\ \ network' = rcv(msg,\, broker)$
        $\land\ \ active' = active \setminus \{msg.from\}$
        $\land$  UNCHANGED $store$
    $\land$ UNCHANGED $pc$
    $\land$ UNCHANGED $topic\_subscribers$
    $\land$ UNCHANGED $used\_num$

$MinQoS(a,\, b) \triangleq$ IF $(a = QoS0 \land b \in\ \{QoS1,\, QoS2\}) \lor (a = QoS1 \land b = QoS2)$ THEN  $a$ ELSE  $b$

$PushMsgsWithQoS0 \triangleq$
          $\land\, Len(network[broker]) = 0$
          $\land \exists\, t \in topics :$
              $\exists\, q1,\, q2 \in \{QoS0,\, QoS1,\, QoS2\} :$
                      $\land\, Len(store[broker][t][q1]) > 0$
                      $\land\, topic\_subscribers[t][q2] \neq \{\}$
                      $\land\, MinQoS(q1,\, q2) = QoS0$
                      $\land$ LET
                              $pId \triangleq Head(store[broker][t][q1])$
                              $subscriber \triangleq$ CHOOSE $one \in topic\_subscribers[t][q2]$ : TRUE
                        IN
                                      $\land\, subscriber \in active$
                                      $\land\, pc[subscriber] =$ “connected”
                                      $\land \exists\, m \in msgs :$
                                            $\land\, m.from = broker$
                                            $\land\, m.type\ = PUBLISH$
                                            $\land\, m.to = subscriber$
                                            $\land\, m.qos = 0$
                                            $\land\, m.topic = t$
                                            $\land\, m.packetID = pId + maxPubNum$
```

```
                                   ∧ canSendTo(subscriber)
                                   ∧ pc[subscriber] = "connected"
                                   ∧ ∨ ∧ Len(store[subscriber]) > 0
                                         ∧ ∀ i ∈ 1 . . Len(store[subscriber]) : store[subscriber][i] ≠ m.pac
                                     ∨ ∧ Len(store[subscriber]) = 0
                                   ∧ network′ = send(m, subscriber)
                                   ∧ store′ = CASE ∀ q ∈ {QoS0, QoS1, QoS2} : topic_subscribers[t][q]
        ∧ UNCHANGED used_num
        ∧ UNCHANGED pc
        ∧ UNCHANGED active
        ∧ UNCHANGED topic_subscribers

PushMsgsWithQoS1 ≜
        ∧ Len(network[broker]) = 0
        ∧ ∃ t ∈ topics :
            ∃ q1, q2 ∈ {QoS0, QoS1, QoS2} :
                    ∧ Len(store[broker][t][q1]) > 0
                    ∧ topic_subscribers[t][q2] ≠ {}
                    ∧ MinQoS(q1, q2) = QoS1
                    ∧ LET
                          pId ≜ Head(store[broker][t][q1])
                          subscriber ≜ CHOOSE one ∈ topic_subscribers[t][q2] : TRUE
                      IN
                             ∧ subscriber ∈ active
                             ∧ pc[subscriber] = "connected"
                             ∧ ∃ m ∈ msgs :
                                   ∧ m.from = broker
                                   ∧ m.type = PUBLISH
                                   ∧ m.to = subscriber
                                   ∧ m.qos = 1
                                   ∧ m.topic = t
                                   ∧ m.packetID = pId + maxPubNum
                                   ∧ canSendTo(subscriber)
                                   ∧ ∨ ∧ Len(store[subscriber]) > 0
                                         ∧ ∀ i ∈ 1 . . Len(store[subscriber]) : store[subscriber][i] ≠ m.pac
                                     ∨ ∧ Len(store[subscriber]) = 0
                                   ∧ network′ = send(m, m.to)
        ∧ UNCHANGED store
        ∧ UNCHANGED used_num
        ∧ UNCHANGED pc
        ∧ UNCHANGED active
        ∧ UNCHANGED topic_subscribers

PushMsgsWithQoS2 ≜
        ∧ Len(network[broker]) = 0
```

```
    $\land \exists\, t \in topics :$
        $\exists\, q1,\ q2 \in \{QoS0,\ QoS1,\ QoS2\} :$
                $\land\ Len(store[broker][t][q1]) > 0$
                $\land\ topic\_subscribers[t][q2] \neq \{\}$
                $\land\ MinQoS(q1,\ q2) = QoS2$
                $\land$ LET
                        $pId \triangleq Head(store[broker][t][q1])$
                        $subscriber \triangleq$ CHOOSE $one \in topic\_subscribers[t][q2] :$ TRUE
                  IN
                                $\land\ subscriber \in active$
                                $\land\ pc[subscriber] =$ “connected”
                                $\land \exists\, m \in msgs :$
                                        $\land\ m.from = broker$
                                        $\land\ m.type\ = PUBLISH$
                                        $\land\ m.to = subscriber$
                                        $\land\ m.qos = 2$
                                        $\land\ m.topic = t$
                                        $\land\ m.packetID = pId + maxPubNum$
                                        $\land\ canSendTo(subscriber)$
                                        $\land\ \lor\ \land\ Len(store[subscriber]) > 0$
                                                $\land \forall\, i \in 1\ ..\ Len(store[subscriber]) : store[subscriber][i] \neq m.pac$
                                            $\lor\ \land\ Len(store[subscriber]) = 0$
                                        $\land\ network' = send(m,\ m.to)$
    $\land$ UNCHANGED $store$
    $\land$ UNCHANGED $used\_num$
    $\land$ UNCHANGED $pc$
    $\land$ UNCHANGED $active$
    $\land$ UNCHANGED $topic\_subscribers$

$HandleRes \triangleq$
    $\lor\ HandlePushQoS1Res$
    $\lor\ HandlePushQoS2Res$
    $\lor\ HandlePubCompRes$

$HandleReq \triangleq$
    $\lor\ HandleConnectReq$
    $\lor\ HandleSubscribeReq$
    $\lor\ HandleUnsubscribeReq$
  $\lor\ HandlePingReq$
    $\lor\ HandlePublishWithQoS0Req$
    $\lor\ HandlePublishWithQoS1Req$
    $\lor\ HandlePublishWithQoS2Req$
    $\lor\ HandlePubrelReq$
    $\lor\ HandleDisConReq$

$PushMsgtoSubscribers \triangleq$
```

$$\begin{array}{l}
\qquad \lor \mathit{PushMsgsWithQoS}0 \\
\qquad \lor \mathit{PushMsgsWithQoS}1 \\
\qquad \lor \mathit{PushMsgsWithQoS}2
\end{array}$$

$$\begin{array}{l}
\mathit{BrokerAction} \triangleq \\
\qquad \lor \mathit{HandleReq} \\
\qquad \lor \mathit{HandleRes} \\
\qquad \lor \mathit{PushMsgtoSubscribers}
\end{array}$$