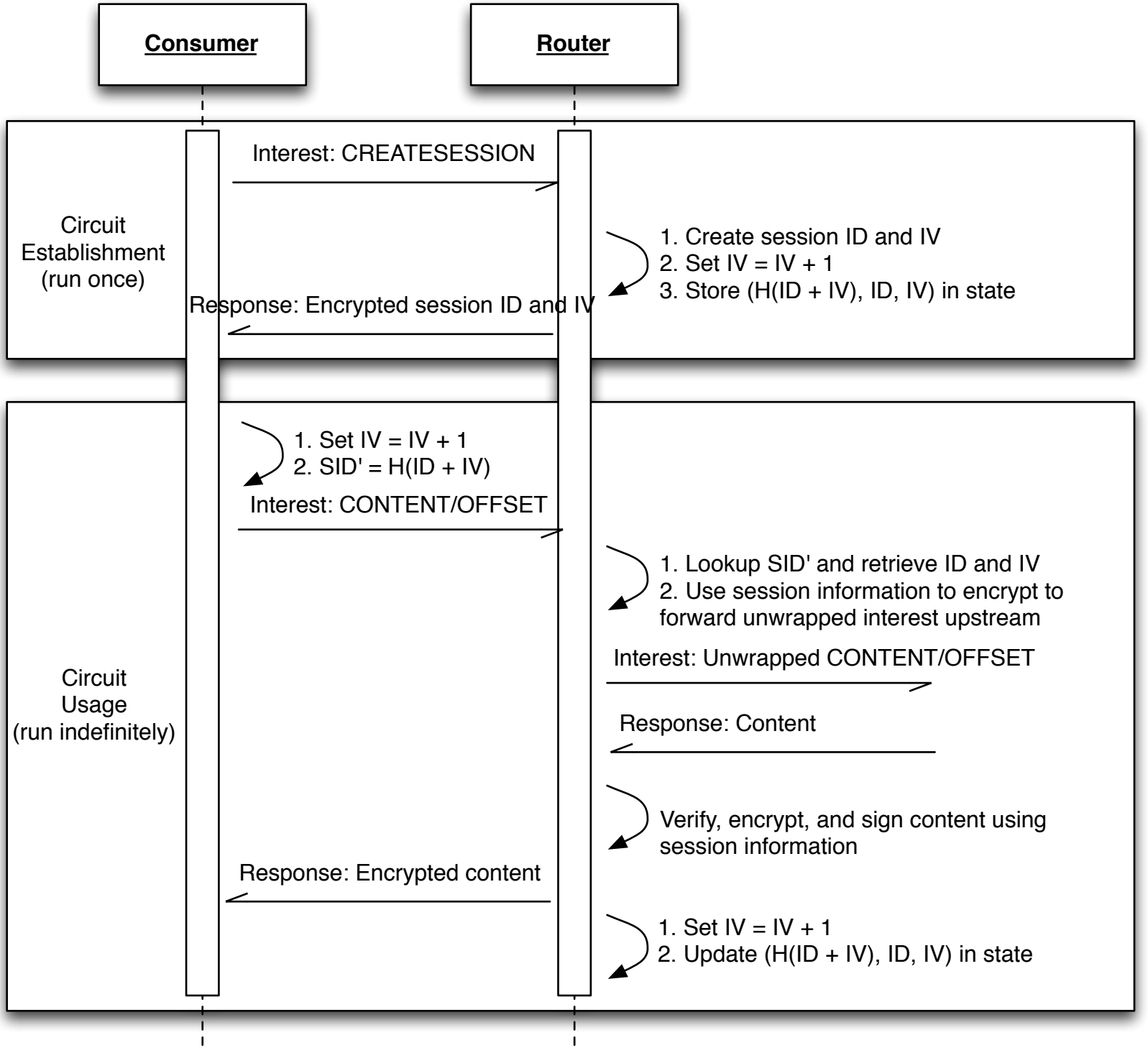
Consumer
Router
Interest: CREATESESSION
Circuit Establishment (run once)
1. Create session ID and IV
2. Set IV = IV + 1
3. Store (H(ID + IV), ID, IV) in state
Response: Encrypted session ID and IV
1. Set IV = IV + 1
2. SID' = H(ID + IV)
Interest: CONTENT/OFFSET
1. Lookup SID' and retrieve ID and IV
2. Use session information to encrypt to forward unwrapped interest upstream
Interest: Unwrapped CONTENT/OFFSET
Circuit Usage (run indefinitely)
Response: Content
Verify, encrypt, and sign content using session information
Response: Encrypted content
1. Set IV = IV + 1
2. Update (H(ID + IV), ID, IV) in state