Motivation

- Client-to-service interaction should not fail when individual servers fail
- Target **Object Delivery Services**:
  - Clients have read-only access to content objects, e.g., webpages, images, and videos
  - Replicated for scalability: 10s to 1000s of servers
  - If one server fails, others can recover its connections

Solution

- Need 2 pieces of information to recover connections
  - **ObjectID** – the object the client is downloading
  - **Offset** – how far the client is into that object
    - e.g., 1200 bytes into /index.html

- Need 2 mechanisms to enable recovery
  - **Persistent Store**
    - Survives server failure
    - Key-Value Store or TCP Timestamp
  - **Recovery Initiation**
    - Leave client’s request unacknowledged, so it times out and retransmits if its server fails

  Implemented as server-side kernel module
  - Clients and server application are unmodified

Insight

We can coerce unmodified clients into retransmitting key information to facilitate recovering object downloads

Evaluation

Throughput is not significantly degraded

Recovery works, cluster throughput is unaffected