Drop Copy Session Layer - Fault Tolerance

Mission critical client applications must continue to function properly despite sudden events such as process termination, hardware failure, or network disconnects. Fault tolerance in a network environment is characterized by rapid recovery from such failures.

One method of providing fault-tolerance is through a mechanism called Failover; the goal is to minimize service interruption caused by error conditions.

Process failure may be caused by hardware failure of the machine on which the process runs, as well as software error; faulty logic, and improper memory handling, among others.

The Drop Copy Gateway initiates a controlled failover when it detects either process or network failure that impacts its ability to service the client.

See the following topics for details regarding each Fault Tolerance error condition and example scenarios:

- Summary of Fault Tolerance Requirements on Client Applications
- Fault Tolerance Implementation
- Fault Tolerance Scenarios
    - Primary Drop Copy Gateway Failure
    - Drop Copy Gateway Outage/Network Failure
    - Drop Copy Gateway Dual Failure

Summary of Fault Tolerance Requirements on Client Applications

The guidelines for implementing fault tolerant client applications are:

- Coordinate applications such that the primary and backup processes each can establish a separate and independent content stream to primary and backup Drop Copy Gateways via TCP/IP socket connection.
- Always set the Fault Tolerance Indicator (FTI) for Drop Copy 4.0 in tag 49-SenderCompID field to 'N' else logon attempt will result in a forced logout.

Fault Tolerance Implementation

Fault Tolerance on Drop Copy 4.0 is managed at the application level.

A client system can only log into and receive acknowledgments through their designated primary connections.

If a client system attempts to log on to the designated backup gateway, while the designated primary gateway is available, CME Globex will send a Logout (tag 35-MsgType=5) message, with tag 789-NextExpectedMsgSeqNum reflecting the value of the next expected sequence number for the designated primary Drop Copy session and tag 58-Text=**Backup session not allowed. Logout forced.**

> Drop Copy 4.0 does not support an active-active fault tolerance connectivity model.

Fault Tolerance Scenarios

Primary Drop Copy Gateway Failure

If the designated primary Drop Copy Gateway fails:

- CME Globex initiates failover by electing the ranking inactive designated backup Drop Copy Gateway to assume the primary role.
- The client application should connect to the newly promoted primary Drop Copy Gateway.
- If the primary connection fails and the client system connects to the newly promoted primary Drop Copy Gateway, that instance will begin with the next available outbound sequence number to the client (outbound sequence number could be higher due to unprocessed in-flight messages).
- Once connected to the new instance, sequence numbers on outbound messages from the client system to Drop Copy must begin with the next available sequence number from tag 34-MsgSeqNum of the previously available Drop Copy gateway instance.
- After failover, Drop Copy may resend previously transmitted messages with tag 97-PossResend=Y on real time messages.

> Upon logging onto the newly promoted primary Drop Copy gateway, the client system can send a Resend Request (tag 35-MsgType=2) message to recover any missed messages. Any missed messages replayed by Drop Copy will have tag 43-PossDup=Y.

Drop Copy Gateway Outage/Network Failure

In the event of network failure or outage, Drop Copy handles socket exceptions that are thrown for network error conditions (i.e., loss of TCP/IP connectivity between the client application and the Drop Copy Gateway). The client system should try to reconnect and logon to the primary Drop Copy Gateway, and if unsuccessful, attempt to connect and logon to the backup.

Drop Copy Gateway Dual Failure

The Drop Copy service provides both a designated primary and backup gateway. In the unlikely event of a CME Group dual component failure, neither the primary nor the backup would be available to service customers.

When the Drop Copy service recovers from a dual failure, the client system should resume sequencing messages with the next available sequence number from tag 34-MsgSeqNum before the dual failure.

Upon recovery from a dual failover, Drop Copy may resend previously transmitted messages with tag 97-PossResend=Y.

If the associated source session initiated an in-session logon during dual failure, only messages transmitted on the iLink source session after the in-session logon will be recoverable.

iLink source session messages transmitted during the dual failure may be recoverable on Drop Copy.