



## **Multiple Master Mirroring for SQL Server Databases**

**and**



## **Single Master Mirroring for SQL Server Databases**

### **WHITE PAPER**

Author: George Kounis  
[gkounis@singleclicksolutions.co.uk](mailto:gkounis@singleclicksolutions.co.uk)

[www.singleclicksolutions.co.uk](http://www.singleclicksolutions.co.uk)

# CONTENTS

<b><u>OVERVIEW.....</u></b>	<b><u>3</u></b>
<b><u>MMM EXPLAINED.....</u></b>	<b><u>4</u></b>
<b><u>SMM EXPLAINED.....</u></b>	<b><u>7</u></b>
<b><u>MMM AND SMM FEATURES.....</u></b>	<b><u>9</u></b>
<b><u>HIGH AVAILABILITY PROVISIONS.....</u></b>	<b><u>10</u></b>
<b><u>Specific Component Protection.....</u></b>	<b><u>10</u></b>
<b><u>Site Protection.....</u></b>	<b><u>10</u></b>
<u>Operator Activated Site Protection Technologies.....</u>	<u>11</u>
<u>Backup and Restore.....</u>	<u>11</u>
<u>Database Snapshots.....</u>	<u>11</u>
<u>SQL Server Log Shipping and SQL Server Replication.....</u>	<u>11</u>
<u>Automatic Failover Site Protection Technologies.....</u>	<u>12</u>
<u>Continuous Availability Technologies.....</u>	<u>13</u>
<u>SQL Server Log Shipping.....</u>	<u>13</u>
<u>SQL Server Replication.....</u>	<u>13</u>
<u>SMM and MMM.....</u>	<u>14</u>
<b><u>WAN TRAFFIC REDUCTION TECHNOLOGIES.....</u></b>	<b><u>14</u></b>
<b><u>MMM and SQL Server Replication.....</u></b>	<b><u>15</u></b>
<b><u>SMM as a WAN Traffic Reduction Solution.....</u></b>	<b><u>15</u></b>

High availability and network speed and capacity have quickly moved to the top of the list of priorities of today's database administrators and business managers.

High availability is a priority because it is no longer acceptable for the enterprise to come to a standstill while waiting for a database restore or for a server to come back on line only to find that data has been lost in the process. Demands on administrators for a restore have moved from several hours down to automatic failover and from some loss of data being acceptable to no loss of data becoming mandatory. Whereas speed of recovery has become essential, fear of terrorism has increased the distance considered safe for keeping recovery copies.

DTI statistics paint the picture:

- 70% of companies go out of business after a major data loss
- 42% of all tape restores fail
- 61% of companies took more than a day to recover from system failures

Network speed and capacity also moved up the list of priorities. The sheer volume of data now being moved on wide area networks and slow connection speeds are constantly increasing the pressure for higher bandwidths and better response times. Organizations, therefore, are caught in ever-increasing spend on WANs when ways to reduce network traffic and increase response times is an obvious alternative.

Multiple Master Mirroring(MMM) and Single Master Mirroring (SMM) for SQL Server now available from Single Click Solutions, address these issues in a very effective way. The intention of this paper is to assist you in understanding how MMM or SMM can provide high availability and lower WAN traffic and how one of these solutions compares with other solutions available in the market.

## **Overview**

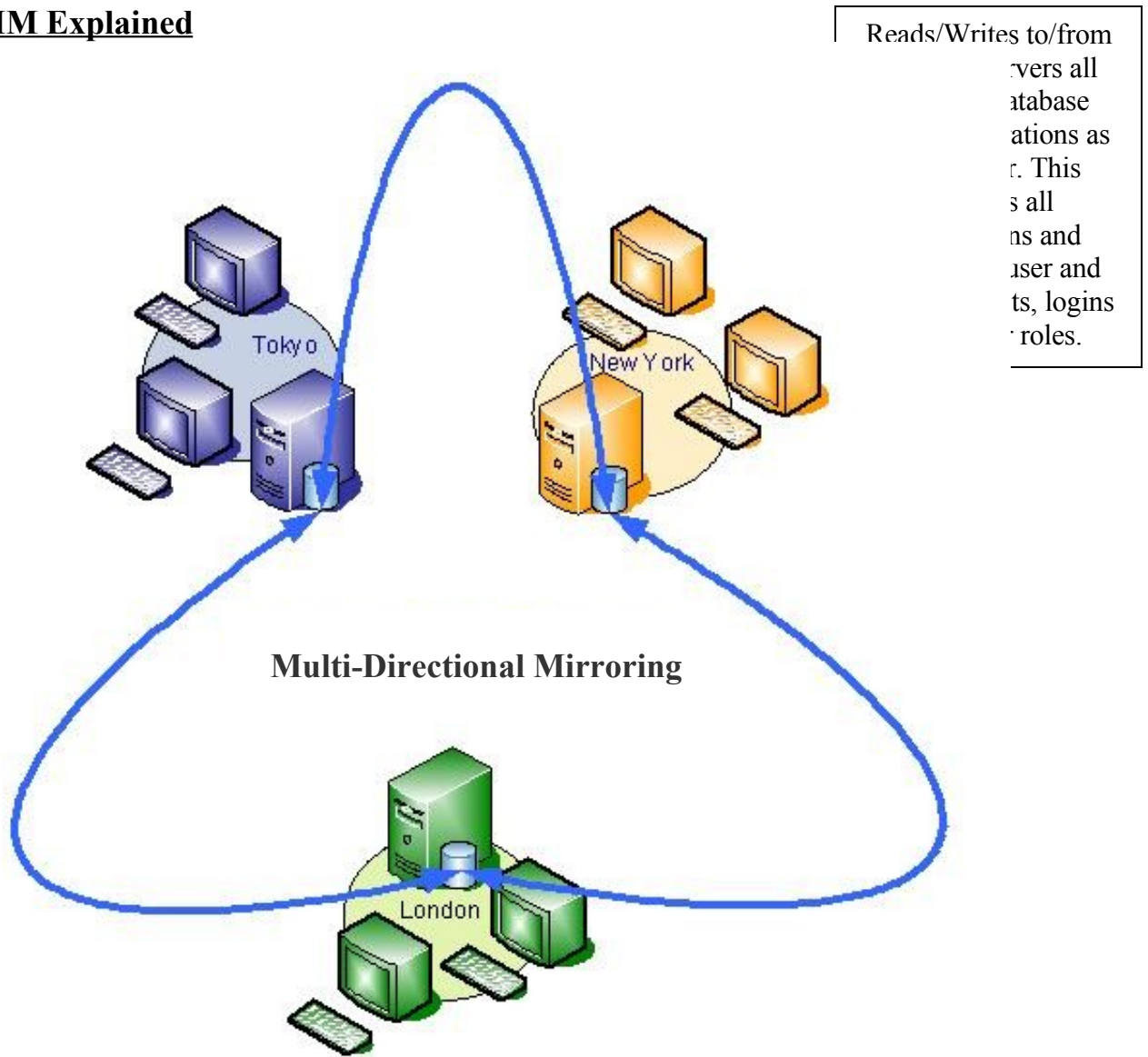
The difference between MMM and SMM is that SMM does one-way real-time database mirroring, whereas MMM allows databases to send and receive changes in real-time.

At the core of MMM and SMM is a logical transaction log reader that replicates as they occur, all DDL and DML operations (i.e. changes to data as well as changes to the database schema). This means that only small bytes of changes are sent through the wire leaving operations that would otherwise tax the WAN to be handled by the LAN thus reducing WAN traffic and latency to a minimum. MMM and SMM, therefore, are the ultimate WAN traffic reduction solutions.

Since MMM and SMM can maintain any number of mirror databases they naturally lend themselves to continuous availability irrespective of a failure in any one of the connected sites. With this in mind, MMM and SMM provide automatic failover and failback as well as automatic redo not only of all operations since the site went down but also of all operations from the point of restoration thus ensuring no loss of data. In this respect, MMM

and SMM are to site protection what clustering is to server protection. MMM and SMM, therefore, are the ultimate continuous availability solutions.

### **MMM Explained**



### Tokyo Site Down

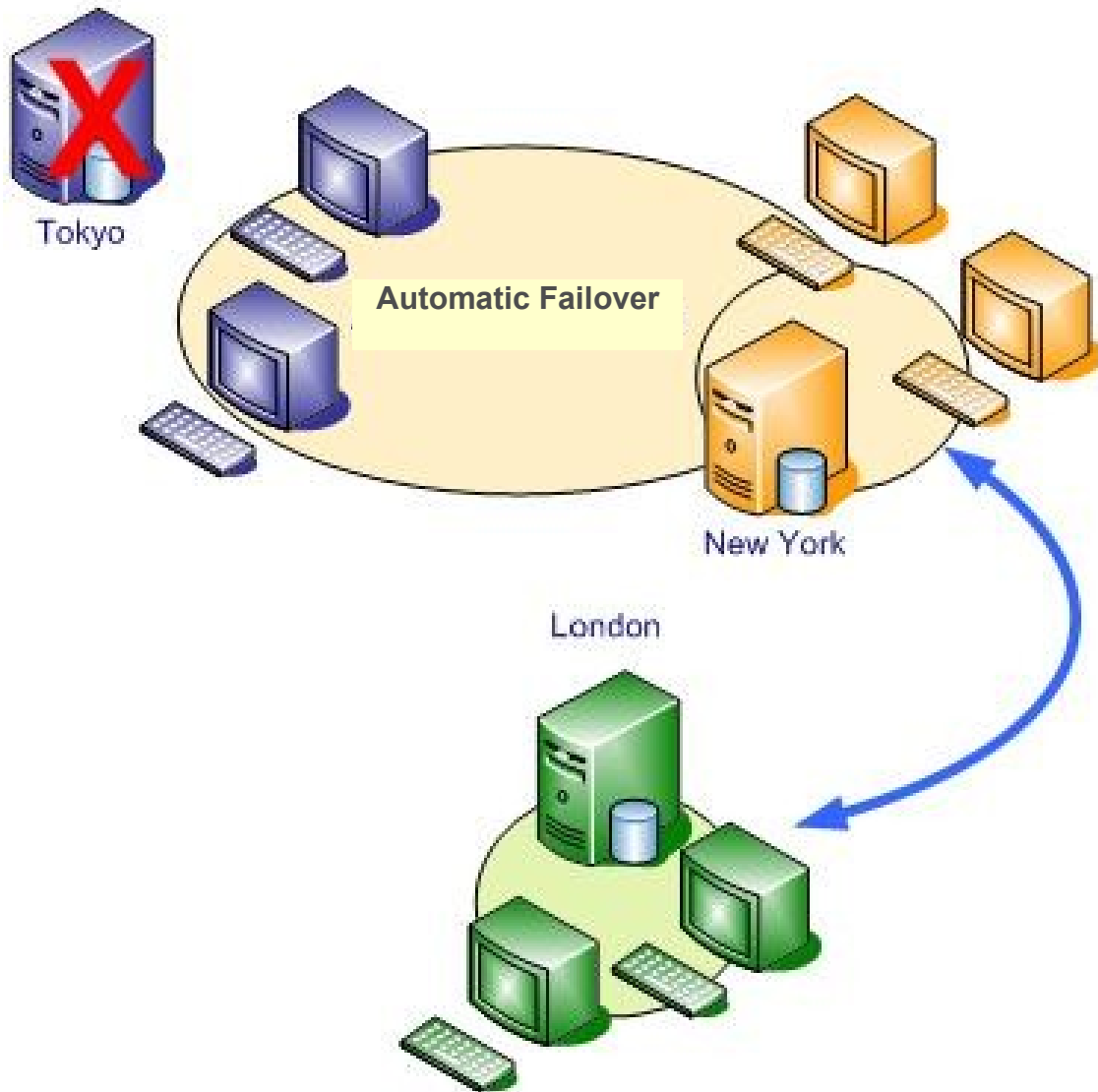


Figure 2

The application also has the facility to switch users automatically to another server in the event of failure of one of the servers.

## Automatic Failback

Tokyo site up again

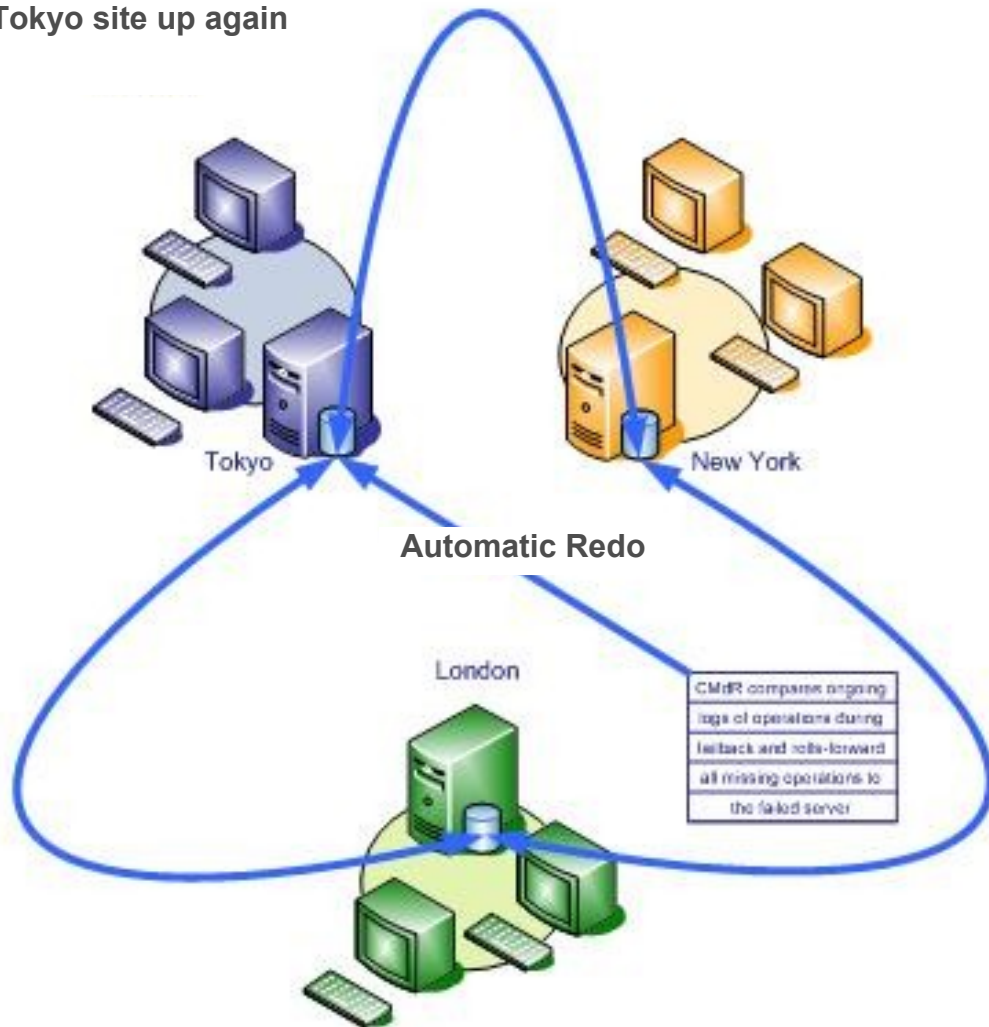


Figure 3

MMM maintains a log of all operations, which allows the application to rewind all operations to the latest backup restored and redo all missing operations to the restored database during failback so that nothing is lost. The ongoing log of operations also provides a complete audit trail.

## **SMM Explained**

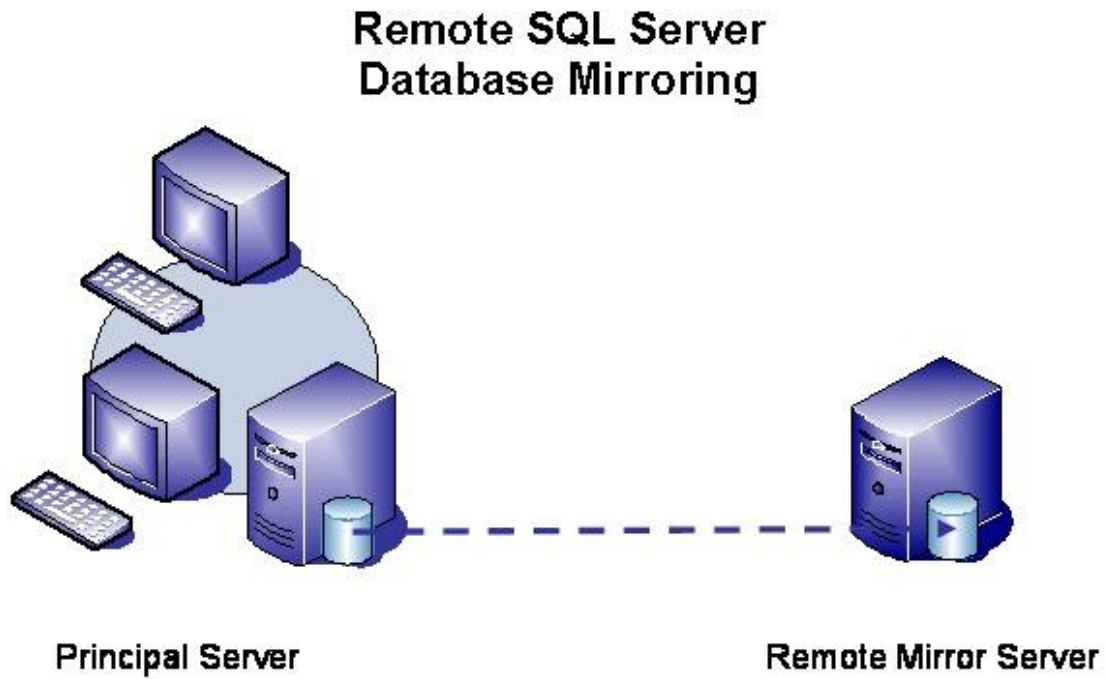


Figure 4

In the event of failure users are automatically switched to the mirror server until the Principal server is restored when the roles are once again seamlessly reversed

## Automatic Failover

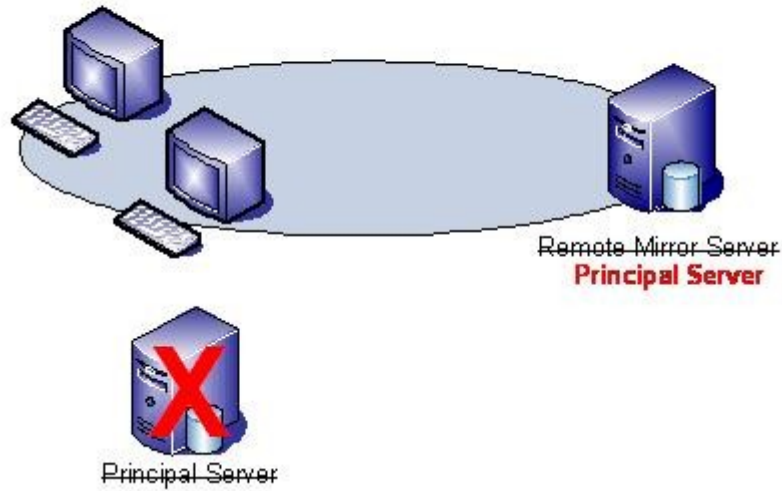


Figure 5

Like MMM, SMM also has the facility to switch users automatically to another server in the event of failure of the Principal. During failover, the Mirror becomes the Principal server. A log of all operations is maintained which allows SMM to re-do all missing operations to the restored database during failback so that nothing is lost. The ongoing log of operations also provides a complete audit trail.

## **MMM and SMM Features**

Send and Receive (MMM)	Will send and receive data and database schema changes to participating databases.
SQL Server 2000 compatible	Will run on SQL Server 2000
SQL Server 2005 compatible	Will run on SQL Server 2005
No Structural changes to tables	Does not involve forcible addition of new table columns to accommodate Replication ID
No database size constraints	No maximum number of columns or rows size in replicated tables
Data and Schema Replication	Replication of all changes in data and database schema as they occur
Low latency	No waiting time between reading from principal and writing to replica.
Corruption Replication Protection	Error log entries are not replicated thus eliminating possibility of passing application corruptions
Conflicting URN Protection	Eliminates possibility that the same URN is allocated to different records from different systems
Unlimited databases and sites	There is no limit to the number of servers and databases that can be replicated by MMM
No distance limitations	Servers involved in replication can be any distance apart
Site failure protection	Provides protection from database, disc, server, connection or any other site failure
False failover protection	Allows administrator to configure when to treat interruption as failover event
Automatic Failover	Switches users to alternative server in the event of failure (subject to connection availability)
Automatic Failback	Switches users back to failed server when recovered
Automatic Redo	Automatic rewind to last backup recovered and redo ensuring no loss of data
Front-end independent FoFa	No need to modify front-end applications for automatic Failover and Failback.
No need for failover witness	Does not require witness to cover exposed mirror during failover
No need for Distributor	Does not require Publisher, Distributor, Subscriber(s) to perform Replication
Asynchronous Mirroring mode	Does not wait for commit from replica thus saving 5-10% overhead in LAN and more in WAN
Mode independent failover	No need to be in synchronous mode for failover
No naming constraints	No need for replicated databases to have the same name
Replicas are in read/write state	Replicated databases are in normal state and can be used for SELECT statements.
Bulk-logged record replication	Replication of bulk-logged operations.
No Recovery Model constraints	Principal database does not have to be in Full Recovery Model to replicate
No need for manual monitoring	No need for DBA to monitor transaction log and log file synchronization.
HCL Independent	Does not require use of components from Microsoft's Hardware Compatibility List
No silent data corruption	Logical groupings of database columns or rows remain intact during replication.

Table 1

## **High Availability Provisions**

High availability provisions aim to reduce or eliminate the effects of failure of one or more of the components that make a database available to users. They can be categorized, therefore, into:

- Those that protect against failure of specific components only; and
- those that protect against site failure as a whole for whatever reason.

## **Specific Component Protection**

Apart from making logistical provisions such as having spare parts available, alternative connections and alternative sites to enable an organization to recover from a failure, technologies that protect against specific component failure include clustering and RAID. Clustering protects against server failure and RAID against disk failure. Both provide automatic failover so that if one server or disk fails the other automatically kicks in.

Neither of these technologies is suitable for site-level protection. The disks in a RAID array need to be in the same location and the cluster nodes can be as far apart as the latency of the storage subsystem will allow (although there is a distance limit of 100 miles). Even if the nodes are set apart at an acceptable distance for site protection, they still need to share the data storage which remains exposed in site-protection terms,

## **Site Protection**

Provisions for site protection are additional and do not aim to replace specific component protection. Here the aim is to consider what would happen if the site becomes unavailable temporarily or permanently for whatever reason. In this respect, we are not responding to the question of what happens if one of the nodes in a cluster or a disk in a RAID array fails. We are asking what happens if the data store becomes unavailable, or, what happens if the WAN connection is interrupted, or, what happens if the site as a whole suffers a disaster.

Site Protection provisions, therefore, necessarily need to facilitate continuity from a remote site. This means one or more servers, connections and availability of the databases at the remote site. There are various methods for making a database available at an alternative site. These may be categorized as:

- those that involve operator intervention which include restoring from a backup and SQL Server database snapshots as well as SQL Server Log Shipping and SQL Server Replication;
- those that provide for automatic failover but the database is not in a usable state unless a failover occurs. SQL Server 2005 Mirroring falls in this category ; and
- continuous availability technologies which provide a usable copy of the database at an alternative location. These can be sub-divided into:

- those that do not provide automatic failover e.g. SQL Server Log Shipping and SQL Server Replication; and
- those that do which include SMM and MMM.

### **Operator Activated Site Protection Technologies**

Operator intervention necessarily means a gap in continuity, the length of which, depends on the technologies used and the provisions made.

#### **Backup and Restore**

This is the traditional way of protecting against any database failure and none of the technologies discussed below are meant to replace the need to take regular backups. Backups are taken periodically and the database is restored from the latest backup. This leaves a gap between the time the backup is taken and the time the failure occurs which may be made up from the transaction log, if the transaction log is still available otherwise all operations that occurred in-between are lost and need to be re-done.

Apart from the backup to failure gap, relying totally on backups may leave even larger gaps depending on the extent of failure. If the whole site has been hit resulting in the non-recovery of the server and/or the data store and/or the backups recovery has to take place to the alternative site from the backup available from that site.

#### **Database Snapshots**

Database snapshots are a new feature in SQL Server 2005 aimed at quick restoration of a database. This technology saves only changes made in the source database to the database snapshot and can be used to restore the source database to the point of time when the snapshot was taken. The facility does not provide server or site-level protection but can protect against application or user database corruption.

#### **SQL Server Log Shipping and SQL Server Replication**

Although when considered under the heading of site protection, they do involve operator intervention before users of a failed site can be switched to the alternative site, the alternative site can continue to be used by other groups of users without any interruption because both Log Shipping and Replication leave the database at the alternative site in a usable state. For this reason, we consider these technologies in more detail under the continuous availability section.

## **Automatic Failover Site Protection Technologies**

### **SQL Server Database Mirroring**

Database Mirroring is a new SQL Server 2005 technology. It is a similar technology to log shipping but unlike log shipping it has automatic failover capabilities. Like log shipping, however, the database is not in a usable state unless a failover occurs.

Unlike log shipping, which allows the use of a time delay for applying transaction logs that can protect against user and application errors, mirroring always sends logs to the mirror as quickly as possible. Furthermore, Database Mirroring cannot discriminate between transactions and will pass application errors to the mirror rendering the mirror susceptible to the same corruption as the principal.

Other disadvantages of SQL Server Database Mirroring are:

- Because the mirror database is in a recovering state, it cannot be accessed directly.
- The principal database must be in the FULL recovery model.
- SQL Server Database mirroring transfers log records directly from the principal to the mirror and cannot deliver bulk-logged data. This is not the case with log shipping where bulk-logged data is appended to a transaction log backup which allows log shipping to work in the bulk-logged recovery model.
- The mirror database must have the same name as the principal database.
- SQL Server Database mirroring cannot be used within a cluster. You may use database mirroring as a method for creating a hot standby for a cluster instance database. Because a cluster failover, however, is longer than the timeout value on database mirroring, a High Availability mode mirroring session will react to a cluster failover as a failure of the principal server. It would then put the cluster node into a mirroring state.
- SQL Server Database Mirroring is limited to a single destination server.
- To have the capability of automatic failover SQL Server Database Mirroring requires modifications to existing applications, a Witness server and to work in synchronous mode. Since in synchronous mode, it waits for commit from replica this adds 5-10% performance overhead in LAN and more in WAN.

## **Continuous Availability Technologies**

Continuous availability technologies provide a usable copy of the database in other locations. Unlike high availability solutions that try to ensure that the same database is available to all users, continuous availability provide usable copies of the database to separate groups of users. Continuous availability schemas can be:

- one peer with many read only subscribers. This includes SQL Server Log Shipping, SQL Server transactional Replication and SMM;
- read/write peers that are subsequently merged. This includes SQL Server Merge Replication; or
- read/write peers that constantly publish their updates to the other nodes. This includes SQL Server 2005 Peer-to-Peer Replication and MMM.

### **SQL Server Log Shipping**

Log shipping is available on the Enterprise Edition of SQL Server 2000 and in all editions of SQL Server 2005. After initializing a secondary server with a full copy of the production database, log shipping uses a SQL Server Agent job to make periodic transaction log backups from the production server and restore them to the secondary server.

Although log shipping can be an effective way of providing high availability to a remote site up to the point of failure, it has no automatic failover facility so recovery has to be done manually.

### **SQL Server Replication**

SQL Server Replication is not primarily aimed at site level protection. They are WAN traffic reduction technologies which lend themselves to site protection due to the nature of what they do.

SQL Server Replication was originally designed to facilitate distributed reporting. Microsoft does not recommend Replication as a high availability solution. It does not provide automatic failover and failback and it does not replicate changes to the database schema (in fact the replicated schema must be identical between the nodes). If you are seeking a high availability solution only, SQL Server Mirroring would lend itself better than SQL Server Replication. It is only if you are seeking a WAN traffic reduction solution that SQL Server Replication may also lend itself for high availability.

## SMM and MMM

Unlike SQL Server Replication, MMM and SMM totally lend themselves to either WAN traffic reduction and/or high availability. With replication of both data and schema changes, automatic failover, re-do and failback, MMM and SMM are the ultimate continuous availability solutions because they provide continuous working, identical copies and no loss of data.

We consider SQL Server Replication, MMM and SMM in more detail below.

## **WAN Traffic Reduction Technologies**

WAN technologies fall into two categories: Those that aim at handling increased traffic by providing higher bandwidths and increased response times and those that aim to reduce WAN traffic altogether. SQL Server Replication, MMM and SMM clearly fall into the latter category.

What accounts for the majority of database traffic are complicated SELECT statements and bulk-logged operations. It follows therefore that if these selections could be carried out locally on database copies the majority of this traffic could be eliminated. This leaves the question of how to update these copies.

SQL Server Transactional Replication lends itself to a read/write peer with read only subscribers which are then synchronized periodically with the peer. SQL Server Merge Replication on the other hand, allows all nodes in the schema to be read/write peers and during synchronization, uses conflict resolution using a pre-defined set of rules about which data changes will be used if the same data is changed at multiple locations. Peer-to-Peer Transactional Replication introduced in SQL Server 2005, treats all nodes as peers and allows each node to publish its updates to the others as they happen.

Transactional Peer-to-Peer Replication does not use the Publisher, Distributor, Subscriber(s) hierarchical structure used by the other SQL Server Replications. Although it is designed for bi-directional replication it does not have the conflict resolution facility provided with merge replication necessitating that data updates are made to different data segments. Due to this Microsoft recommends that either the servers are separated into read only servers and a read/write server or ensuring that the peers span a significant time zone difference, and thus no overlaps occur in write activity when contentions may occur.

## **MMM and SQL Server Replication**

SQL Server Replication has several disadvantages over MMM:

- SQL Server Replication necessarily involves the addition of new table columns within the application's database and/or you need to manage your identity columns, forcing an automatic and non-configurable modification to the underlying database schema. This may interfere with support agreements and complicates future upgrades.
- SQL Server Replication does not replicate database schema changes and the replicated schema must be identical between the nodes. The system, therefore, would need to be quiesced (stopping activity on published tables at all nodes and ensuring that each node has received all changes from all other nodes) whenever the schema changes.
- Tables used in SQL Server merge replication can have a maximum of 246 columns and a maximum row size of 6,000 bytes which could be a constraint in certain cases.
- The Microsoft merge replication architecture is based upon an initial and periodic snapshot-and-restore process to re-synchronize the sites in the network. Although the snapshot creation and application process is largely automated these snapshot files can be very large and require adequate storage and the process can be very time consuming and cause unnecessary 'downtime'.

## **SMM as a WAN Traffic Reduction Solution**

If the requirement is for distributed reporting whereby the mirrors will only be read then SMM is the ideal solution. It has all the facilities of MMM except multi-directionality and, if required, it can lend itself as a high availability solution which in conjunction with normal backup routines may provide a complete failsafe solution providing continuous availability and ensuring no data loss.

## Solution Comparison

Features	Log Shipping	Database Snapshots	Database Mirroring	Replication Transactional	SMM	Merge Replication	Peer-to-Peer Replication	MMM
Send and Receive	X	X	X	X	X	√	√	√
SQL Server 2000 compatible	√	√	X	√	√	√	X	√
SQL Server 2005 compatible	√	√	√	√	√	√	√	√
No Structural changes to tables	N/A	N/A	N/A	X	√	X	X	√
No database size constraints	N/A	N/A	N/A	√	√	X	X	√
Data and Schema Replication	√	√	√	X	√	X	X	√
Low latency	√	√	√	X	√	X	X	√
Corruption Replication Protection	X	X	X	X	√	X	X	√
Conflicting URN Protection	N/A	N/A	N/A	N/A	√	X	X	√
Unlimited databases and sites	√	√	X	√	√	√	√	√
False failover protection	X	X	X	X	√	X	X	√
Automatic Failover	X	X	√	X	√	X	X	√
Automatic Failback	X	X	√	X	√	X	X	√
Automatic Redo	X	X	X	X	√	X	X	√
Front-end independent FoFa	N/A	N/A	X	N/A	√	N/A	N/A	√
No need for failover witness	N/A	N/A	X	N/A	√	N/A	N/A	√
No need for Distributor	N/A	N/A	N/A	X	√	X	√	√
Mode independent failover	N/A	N/A	X	N/A	√	N/A	N/A	√
No naming constraints	X	X	X	X	√	X	X	√
Replicas are in read/write state	√	X	X	√	√	√	√	√
Bulk-logged record replication	√	√	X	√	√	√	√	√
No Recovery Model constraints	√	√	X	√	√	√	√	√
No need for manual monitoring	√	√	X	√	√	√	√	√
No silent data corruption	√	√	√	X	√	X	X	√

\* See Page 9 for a complete List of Features and an explanation of each feature.