Payment Authorization –
A Journey to Continuous Availability

A Gravic, Inc. Case Study

Executive Summary

A major provider of merchant services to over four million small to medium-sized businesses throughout the world provides payment authorization for Visa, MasterCard, American Express, Discover, Diners Club, and other credit and debit cards. Card transactions made at merchant point-of-sale (POS) devices and ATMs are verified to ensure that they are non-fraudulent.

The company's payment authorization services are extremely critical. If any of these services becomes unavailable, then shoppers all over the world will not be able to use their credit or debit cards. Therefore, the company has worked diligently to guarantee that its authorization services will always be available via data replication technology.

Over a period of several years, as the company learned the benefits of data replication, it expanded its use of data replication technology from disaster recovery to active/active systems to application integration in a measured and careful process. Today, this effort has resulted in a system that is continuously available and integrated with other IT services.

Payment Authorization

Credit and debit cards are issued by banks and are used by consumers to purchase items from brick-and-mortar and online stores and to withdraw cash from ATMs. Each card transaction must be approved by the issuing bank before it can be accepted by a merchant or by an ATM. The payment authorization process begins when a consumer's credit card is presented for payment, which might occur at a POS device, such as a credit-card reader connected to a store's cash register. It might be initiated when a consumer gives his credit card number and other information to a sales person over the phone or when this information is entered into a website form.

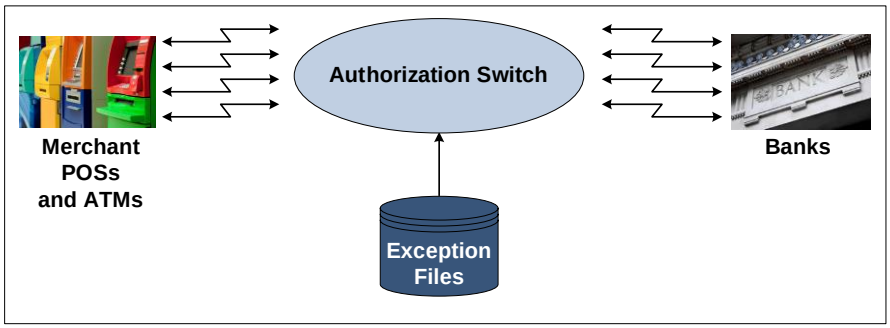

Figure 1 – Merchant Authorization Services

A communication channel to an authorization switch established and managed by an organization providing merchant services connects the POS device, the ATM, or the system hosting the sales support for phone or online ordering. As shown in Figure 1, the authorization switch receives the transaction and analyzes it, determines which bank is servicing the credit or debit card, and sends the transaction to that bank. It will check if the card has been lost or stolen and may check the transaction for suspicious charge activity.

If the bank responds positively, and if the switch detects no other problems, an authorization message is returned to the originating device or system. If the bank rejects the transaction, if the card has been reported as lost, stolen, or frozen, or if the transaction is suspicious (i.e., a potentially fraudulent use of the card), the transaction is rejected.

A Start with Disaster Recovery

The merchant services provider operates a major authorization switch in North America, and its two data centers are 1,000 miles apart on the East Coast of the United States, named Center North and Center South. The switch functions are duplicated in each data center to provide recovery from any disaster that might take down one of the provider's data centers. In normal operation, the processing load is distributed between the two sites.

The company's first use of data replication was to keep the Card Management Application (CMA) systems in each data center synchronized. Hosted on HPE NonStop servers, the CMA systems provide a database of all cards issued by participating banks, including Visa, MasterCard, American Express, Discover, Diners Club, and other cards.

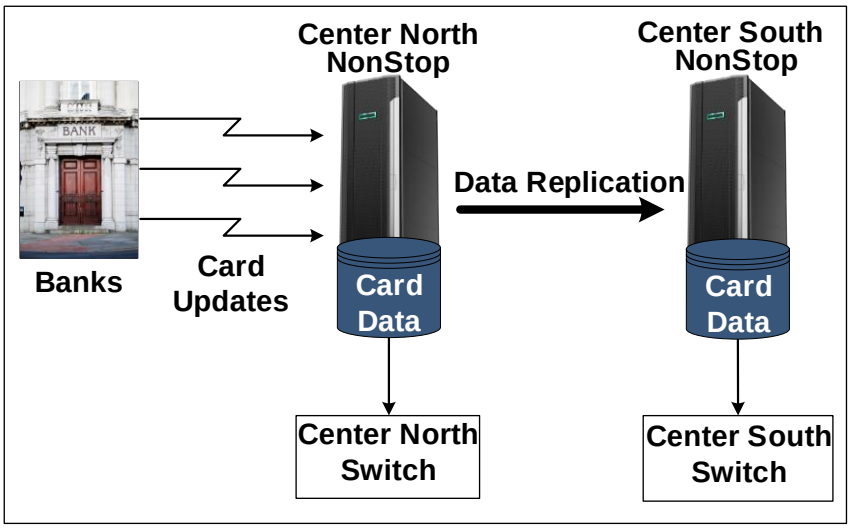

Figure 2 – Card Management Applicator (CMA)

Banks send batch ftp files to the CMA system for new cards they issue, cards they report as stolen or lost, and other card status changes. These batches are received by the Center North CMA system and stored in its card database. This database is then replicated to the Center South CMA system via the HPE Shadowbase data replication engine (Figure 2). Therefore, both CMA systems always have the complete and up-to-date data of all cards that have been issued.

The CMA database specifies which issuing bank services each card, what the card's characteristics are (its card number, its expiration date, its credit limit, its PIN, and so on), and its status (active, lost, stolen, frozen, and so on). Additions and changes to this database are sent by each CMA system to the switching nodes nearest to it. Therefore, each switching node has direct local access to all card data, a requirement for fast authorization. Fast authorization is necessary so that a customer does not have to wait long while the transaction is completed, and the POS, ATM, or telephone sales clerk can then service the next customer.

By maintaining a copy of the CMA database at each site, the company ensures that the CMA data is available at all times, even in the event of the failure of one of the systems. If one system fails, then all batch updates from the issuing banks will be routed to the other CMA system; and this system will be responsible for keeping the nodes at both sites updated.

This architecture also allows rolling upgrades to be made to the CMA systems. One system can be taken down and its operating system, application, database, or hardware upgraded while the other system carries the CMA load. The first system can then be returned to service and the second system taken down for upgrade.

The Move to Active/Active

After several years of successful operation with the disaster recovery configuration for the CMA systems as described above, the service provider moved to an active/active configuration for its authorization switch. The switch contains four nodes – two in Center North and two in Center South. Each node is connected to thousands of communication lines that connect to the company's massive IP network. When a transaction is received from a merchant, the job of the switch is to validate the card/transaction, route it to the issuing bank, and then to return the response to the merchant.

Switch Configuration

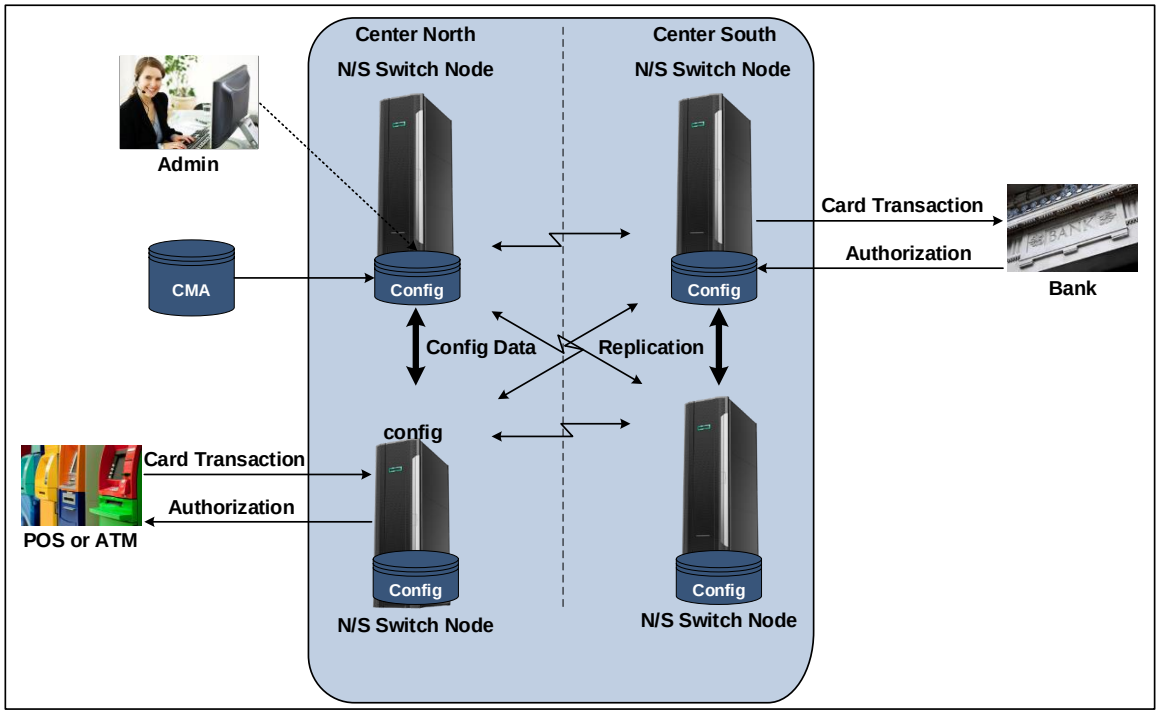

Figure 3 – Active/Active Authorization Switch

Though all switching data is kept in memory, the switch configurations are kept on disk in a configuration database. The configuration database also contains failover configurations so that surviving nodes can take over the functions of a failed node. Consequently, the configuration database is fundamental to proper switch operation. A copy of the configuration database is maintained on each node for local access. These copies are kept synchronized by the Shadowbase bi-directional data replication engine (Figure 3).

The card number partitions the credit and debit cards across the nodes. Consequently, each card is "owned" by one of the nodes, which prevents data collisions occurring on card updates due to transaction activity. All transactions for a card are routed to the node owning that card; the node makes transactional updates to its database, and Shadowbase software replicates the changes to the other database copies in the network. No two nodes are making simultaneous changes to a card due to transaction activity, and data collisions are avoided.

Transaction Processing

When a transaction for a card is initiated, the authorization switch's IP network routes the transaction to the node owning that card based on the card number range reflected in the transaction. When its owning node receives a card transaction request, the configuration database is accessed to determine which bank issued that card and should receive the transaction. The configuration database specifies the IP address of the issuing bank, and the owning node forwards the transaction request to that bank.

When the issuing bank returns a response to a transaction request, the company's IP network returns that response to the node owning the card. An authorization or rejection message is sent by the owning node to the initiating device to complete the transaction. The transaction is authorized if the issuing bank authorizes it and if the authorization switch has detected no other problems, as described later (lost or stolen card, frozen card, suspicious activity, and so on).

Node Failover

Equally important is the failover configuration data maintained in the database. If a node fails, the configuration database tells the surviving nodes which cards are their responsibility. The surviving nodes then assume ownership of their newly assigned cards so that switching services can continue. The configuration failover database also tells each node which applications it should take over to continue operations. All cards that are

owned by the failed node are switched to surviving nodes, as are the failed applications. Authorization services continue without interruption. In fact, this procedure is repeated for multiple node failures so that operations can continue even if more than one node fails.

Replicating Changes

The redistribution of cards, card transactions, and applications to surviving nodes is one of the requirements for an active/active system. Equally important is that each node must have a current copy of the application database. In the case of the authorization switch, there is no real-time data to be replicated since it is all kept in memory. If a node fails during transaction processing, the originating system will time out, resubmit the transaction, which the new node configuration will process.

However, there must be a current copy of the configuration database resident at each node. The configuration database is accessed and may be updated during each transaction or modified by administrative operators. In addition, card changes are received from the CMA system. All of these changes are replicated to each of the other nodes by the Shadowbase data replication engine so that each node has a current copy of the configuration database.

Though transactional changes to a card are made only by its owning node and are replicated to the other nodes from that node, administrative changes to a card may be made at other nodes. Of course, these changes open up the possibility of data collisions if a change to the same credit or debit card is made at two different nodes almost simultaneously (within the replication latency interval). This scenario is unlikely due to the nature of the card partitioning, however, if there is a collision, the company's data collision resolution algorithm (implemented in a Shadowbase user exit procedure) accepts the later change, and the other change is rejected and logged for subsequent manual review.

The Shadowbase data replication engine performs another important function. As the failover configuration is modified (which it must be for every new card), the update is entered with respect to the node receiving the configuration updates. However, this configuration data is different for each node, since each node will take a different action on failover. For instance, node 1 might handle card A. If node 1 fails, node 2 might handle card A. If node 2 then fails, node 3 might handle card A. By applying specific business rules, the Shadowbase engine automatically adjusts the configuration data for each node as it replicates the data.

Therefore, the company converted its four-node switch to an active/active configuration which will recover almost instantly from any fault in the system, including a total node (or multinode) failure, with recovery transparent to the users.

Heterogeneous Application Integration

A major function of authorization is to detect the fraudulent use of cards. If a transaction looks suspicious – for instance, it is for a purchase in a New York store whereas the last transaction one hour ago was for a purchase in a Los Angeles store – it may be rejected.

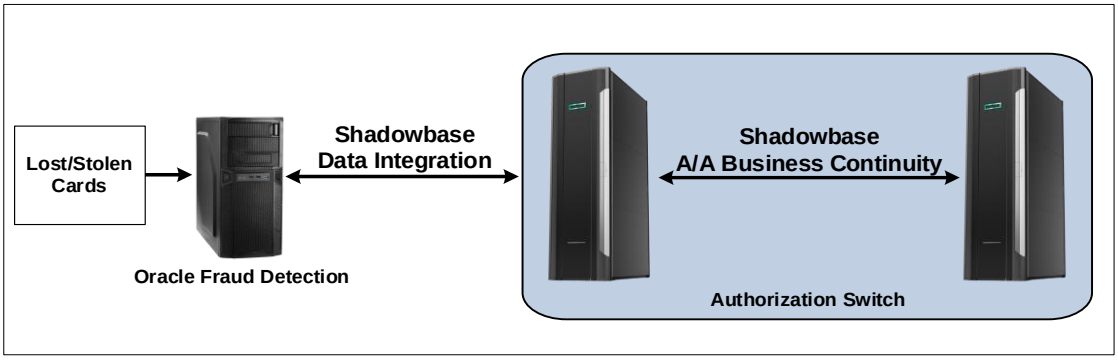

Figure 4 – Fraud Detection

As shown in Figure 4, the company implemented a fraud detection application using an Oracle fraud detection system, where each transaction received by the authorization switch is sent to the Oracle system that maintains a log of recent transactions and checks them against other recent transactions for the same card. If a transaction appears to be suspicious, the result is passed to the authorization switch, which may then reject the card's transaction. The switch may also notify the issuing bank of its action; and the bank, at its discretion, may freeze the card. The cardholder is notified and must call, verifying both credentials and recent transactions.

The fraud detection system is also periodically sent a list of cards that have been reported lost or stolen or that have been frozen by the issuing bank. If a transaction is made against such a card, this situation is reported back to the switch, which will reject the transaction.

The Integrated Authorization Switch

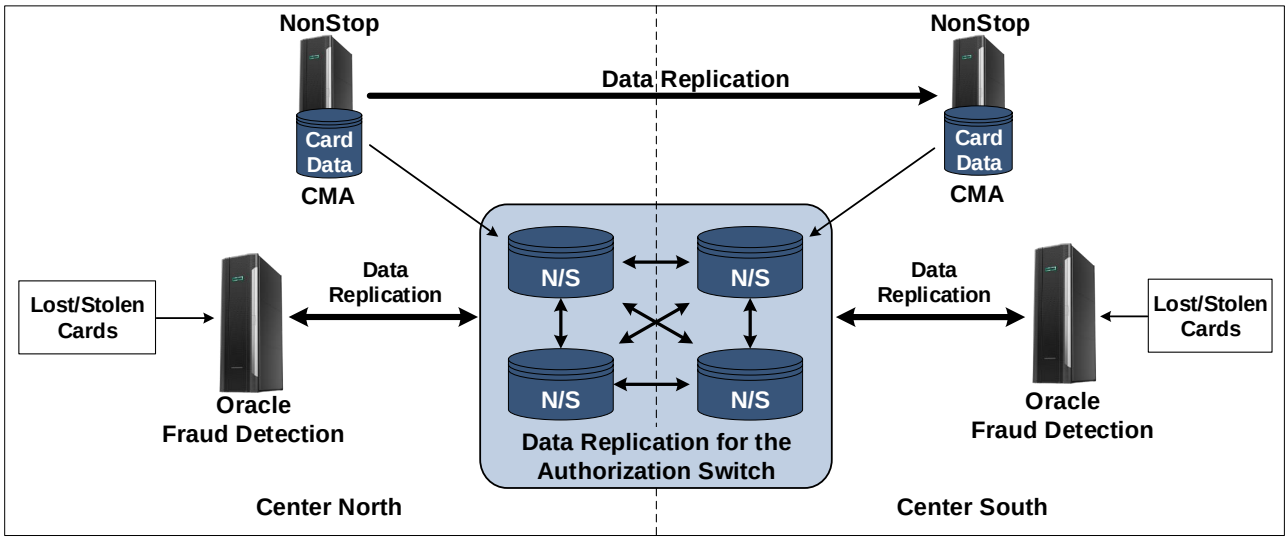

Figure 5 – Integrated Authorization Payment Switch

As shown in Figure 5, at each data center there is one fraud detection system serving the nodes at that site. The company implemented communication between the fraud detection system and the authorization switch nodes using the HPE Shadowbase engine. When a transaction is received, a notation is made in the card's database on the authorizing switch. This notation is replicated to the fraud detection system, where Shadowbase replication detects the request as it updates the Oracle database. The request is passed via Shadowbase application integration to the fraud detection application, which logs a response by updating its database. When Shadowbase software replicates this change back to the authorization switch, the response is detected and passed by Shadowbase application integration to the authorization switch's switching logic. Consequently, either the authorization switch receives a transaction authorization or a rejection notice from the fraud detection system in real-time. This architecture is an example of Shadowbase heterogeneous application integration, since the authorization switch nodes are HPE NonStop systems and the fraud detection systems are Unix/Oracle-based.

The authorization switch maintains its own database – an exception file – of all cards against which transactions were initiated and reported as lost, stolen, frozen, or rejected by the switch due to suspicious activity. A card is cleared from this list when the issuing bank notifies the switch during one of its batch updates of card changes.

The authorization switch is heavily involved in the authorization decision. When it receives a transaction, it first checks its exception file. If the card is not listed in this file, the switch sends the transaction to the fraud detection system and to the issuing bank. The originating device is notified to accept the transaction if all of the tests are positive: it is not in the exception file or suspicious, and the issuing bank authorizes it. If these tests fail, then the originating device is instructed to reject the transaction.

Summary

This merchant services company carefully expanded its use of HPE Shadowbase data replication over the years. The company initially used it to provide a uni-directional active/passive data recovery capability for its CMA. After feeling comfortable with this use of data replication, the company expanded its use of Shadowbase technology to provide continuous availability for its multinode switch. Finally, it integrated heterogeneous applications (the fraud detection system) via Shadowbase data replication and heterogeneous application integration. This case study demonstrates the many uses of HPE Shadowbase software in mission-critical applications.

International Partner Information

Global

Hewlett Packard Enterprise
6280 America Center Drive
San Jose, CA 95002
USA
Tel: +1.800.607.3567
www.hpe.com

Japan

High Availability Systems Co. Ltd
MS Shibaura Bldg.
4-13-23 Shibaura
Minato-ku, Tokyo 108-0023
Japan
Tel: +81 3 5730 8870
Fax: +81 3 5730 8629
www.ha-sys.co.jp

Gravic, Inc. Contact Information

17 General Warren Blvd.
Malvern, PA 19355-1245
USA
Tel: +1.610.647.6250
Fax: +1.610.647.7958
www.shadowbasesoftware.com
Email Sales: shadowbase@gravic.com
Email Support: sbsupport@gravic.com

Hewlett Packard Enterprise Business Partner Information

Hewlett Packard Enterprise directly sells and supports Shadowbase Solutions under the name ***HPE Shadowbase***. For more information, please contact your local HPE account team or visit our website.