



NEC Solutions America

**Disaster Recovery:  
The Only Choice for  
Mission-Critical Operations  
and Business Continuity**

NEC Solutions (America), Inc.  
2890 Scott Boulevard  
Santa Clara, CA 95050  
[www.necsam.com](http://www.necsam.com)

## Introduction

The importance of having uninterrupted access to business data and applications is nothing new. "Availability" has become such a vital aspect of doing business in today's world that it is no longer even a buzz word. It is an imperative. And with the proliferation of network computing—not only network-accessible data, but network-accessible applications as well—"availability" has begun to take on a whole new meaning. It has become important to protect more than just your data. The applications and infrastructure that allow users to *work* with that data must also be protected. Compound the hazards of local hardware failure with the potentially debilitating (if not fatal) financial blow that could be dealt to an organization by a natural catastrophe or an act of terrorism, and the importance of having a sound disaster recovery solution in place becomes incredibly clear.

This paper discusses today's options for ensuring business continuity by protecting mission-critical data in the event of the destruction of local computing resources and how NEC's solutions can provide every company with an affordable way to allow surviving resources to continue working with access to the latest data after a disaster.

## Protecting Mission-Critical Information

Depending on how servers are being used, the cost of an hour of downtime can reach hundreds of thousands of dollars. In the financial services industry, for example, applications related to brokerage operations or online credit card sales authorization can incur millions of dollars per hour of downtime.

### Industry Downtime Costs

Application	Cost per minute
Call location	\$27,000
Number portability	\$14,400
ERP	\$13,000
Supply chain management	\$11,000
Electronic commerce	\$10,000
Internet banking	\$7,000
Universal personal services	\$6,000
Customer service center	\$3,700
ATM/POS/EFT	\$3,500
Messaging	\$1,000

Source: *The Standish Group International, Inc.* © 2001

While it may have been 9/11 that brought disaster recovery to the foreground as an IT issue, occurrences like earthquakes, floods and tornados are threats that have been with us forever. And their potential impact is magnified with ever-increasing reliance on systems that are prone to be severely, if not irreparably, damaged by them.

For all these reasons, disaster recovery is an important topic for IT executives today. In a recent Forrester survey, over 50% of executives from manufacturing companies surveyed considered an initiative to upgrade their disaster recovery utilities to be a major theme for their organization to address in 2004. This ranked as the number one initiative that respondents mentioned. *[Source: Forrester's Business Technographics® November 2003 North American Benchmark Study]*

The challenge has become for IT executives to first and foremost protect mission-critical data in the event of the destruction of local computing resources, and further, to ensure that surviving personnel will have the means to continue working with that data. And to do so cost-effectively and without sacrificing the level of attention and resources allocated to other IT priorities facing the organization.

To help provide some guidance, the Securities Industry Association (SIA) recently released their "Continuity Guidelines" for organizations in the securities industry, which states:

- Each firm should have in place a Business Continuity Program that includes prevention and mitigation activities that reduce the likelihood and impact of business disruption.
- Recovery facilities should not be located in the same geographical zone as the primary business facility and should be supported by separate telecommunication and utility infrastructures.

*[Source: [www.sia.com/business\\_continuity/pdf/bestpractices.pdf](http://www.sia.com/business_continuity/pdf/bestpractices.pdf)]*

To this end, NEC has developed a complete, cost-efficient disaster recovery solution that will provide a solid foundation for the Business Continuity Program of any organization that relies on its IT infrastructure for success.

## **Disaster Recovery Solutions**

Before introducing NEC's solution, it is important to set the stage by outlining the two "traditional" approaches to disaster recovery that have emerged in recent years for small/medium enterprises: Data Replication and Clustered Servers.

The Data Replication approach involves making timely and regular copies of critical data to a remote location. This is accomplished either with a direct connect tape backup and relocation of the tape to another outside location, or with disk to disk replication from server to server, and in some cases a combination of the two (with tape backups being made for archiving purposes and disk to disk backups being made for disaster recovery purposes). In the event of a disaster, the data is restored to the primary system from backup once the disaster has ended and if necessary,

once the primary system has been repaired. While these solutions are relatively cost-effective and do protect the data, they do not protect the applications, and recovery time can be fairly significant. Furthermore, any data created or updated between the disaster and the last backup is lost—a major drawback for systems that host thousands of transactions per day.

The Clustered Server approach involves linking two servers (located at different sites) with cluster software. The servers share one data repository, and each has its own copy of the Operating System [OS] and applications. In the event of a disaster at one site, all user traffic fails over to the instance of the applications residing at the other location. To restore the system to a "disaster-tolerant" state, the downed system must then be painstakingly reintroduced into the cluster.

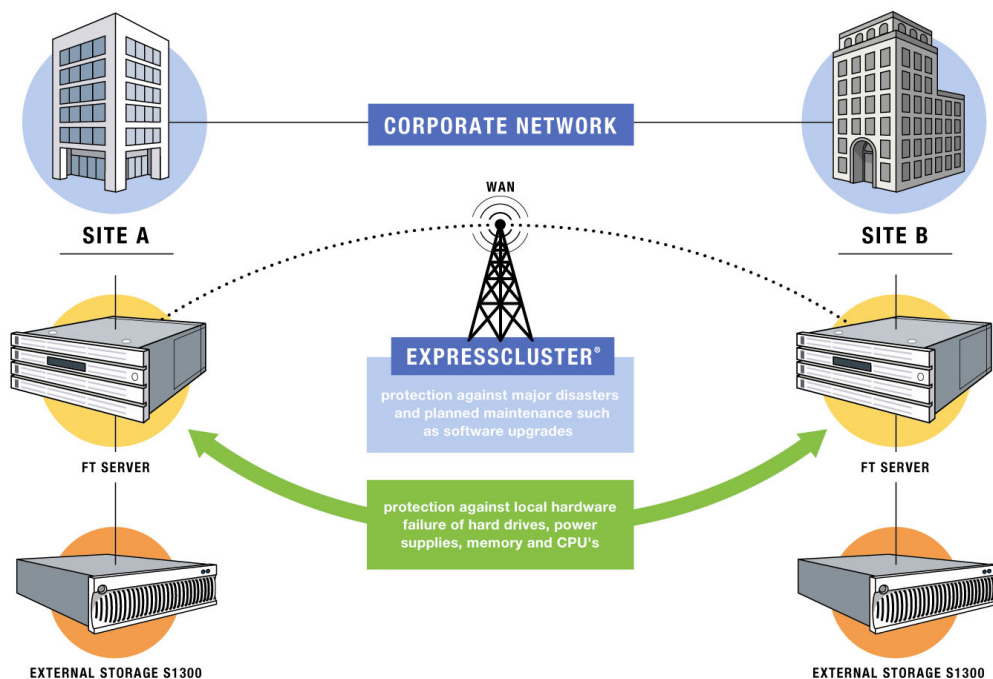
This approach has the advantages of protecting the applications and operability (as opposed to only the data), and allowing users to be up and running again within several minutes. However, it also has a number of distinct disadvantages. First, to maximize the availability benefits of clustering, all applications must be "cluster aware"—i.e. they must be designed to operate in a clustered environment—limiting the applications the organization has the option to use. Second, these clusters are more complex and difficult to configure and administer than a single system. Failback is as much work as the initial set-up. As a result, they require more sophisticated IT resources than an organization might otherwise require. Third, the clustering software currently available that enables a synchronous remote mirroring solution is only able to connect two sites that are up to a couple dozen miles apart—a distance likely to be insufficient to isolate one site from a disaster occurring at the other. Finally, one of the most significant challenges that an IT department faces is complexity and difficulty of disaster recovery system integration. Typical disaster recovery solution deployments require multi-vendors technologies, products and services consisting of servers, storage, data replication mechanisms, system and application monitoring, and failover/failback mechanisms. It requires significant volume of integration efforts.

## The NEC Solution

### *Architecture/Overview*

NEC's unique disaster recovery solution circumvents the disadvantages of the alternatives cost effectively, and also provides significantly enhanced protection from local hardware failures, by utilizing NEC's state-of-the-art fault tolerant (FT) servers—the only servers on the market today that offer total hardware redundancy without clustering, by including two constantly-monitored, automatically-switching sets of hardware in the box. This ensures that both data and applications are protected on two levels—first locally and second over the WAN. The solution begins with an NEC Express5800 FT Server and an NEC S1300 storage module at each of two locations. Each server hosts a complete instance of the applications required by users. Under normal conditions, the users at one site utilize the instance of the applications on their server, as do users at the second site—not entirely unlike the clustered server approach.

But with the NEC Disaster Recovery Fault Tolerant (FT) Solution, rather than accomplishing data redundancy by way of rolling backups, the data is kept in synch between the two sites continuously by virtue of the fact that every transaction written to one server is simultaneously written to the other server, via a dedicated network connection between the sites. In a disaster, if data and/or application resources are compromised at one location, the users at the other location will be unaffected, while the users at the "problem location" will be automatically logged out. Upon logging (immediately) back in, they will begin working from the instance of the applications at the other site, and continuing to utilize up-to-date data.



When the disaster is over, and the downed site's server is brought back online, the system will automatically begin re-synching the data on that server with the data on the other server. Once the re-synching is complete, after a quick log-out—which can be easily configured to either occur automatically or be scheduled by IT personnel to occur at a convenient time—and re-log-in, users will return to working with the instance of the applications residing at their home site.

This approach eliminates the disadvantages of the data replication solution by protecting the applications (not just the data), reducing down time and recovery time to that of the few minutes it takes to log back in, and ensuring that users are constantly working with up-to-date information.

NEC's solution similarly eliminates the disadvantages of clustered servers. Unlike traditional clusters, NEC's solution does not require applications to be "cluster aware", hence freeing IT personnel to utilize whatever applications best suit their users' needs. It is more straightforward to set up and maintain than traditional clustering. It supports distances of a few hundred miles or more between the two sites, depending on bandwidth and latency, rather than limiting that distance to a couple dozen miles. Failback is as simple as logging back in. And the processor and network overhead of rolling backups is eliminated.

This solution is offered as a complete package that includes all the hardware, software and services necessary to implement this system quickly and cost-efficiently.

### *Requirements*

Each FT server must be allocated two network connections—one for regular network traffic, and another called Interconnect to maintain synchronization between the two servers. The Interconnect must be a dedicated WAN connection with at least T1 speed, and the two sites must be located within a few hundred miles of one another, depending on bandwidth and latency. Greater distances may be achieved with a faster connection and/or if increased latency is acceptable. Each FT server must have a S1300 storage module attached for database storage/archive; the two servers must share the same "Floating Name and Floating IP Address" on the VLAN environment; and there must be the ability to tunnel Ethernet packets over the WAN.

For organizations with users at only one location, an "active/passive" configuration may be implemented, utilizing an FT server at the user site and a general purpose server at the remote location. In this configuration, constant synch is still maintained and users still fail over to utilize applications and up-to-date data on the remote server, as described above. The only differences are that no users utilize the remote server under regular conditions, and that the performance/cost requirements for that remote server are therefore decreased.

## *Hardware*

At the heart of the Disaster Recovery (FT) Solution is the Express5800/320Lb Fault Tolerant (FT) server. As referenced earlier, this server provides total hardware redundancy without clustering. Each FT server has two CPUs, two chipsets, two sets of memory, and two sets of PCI I/O hardware—all constantly monitored by native fault detection processes, which automatically fail over one or more hardware components to their counterparts as necessary.

This configuration eliminates all single points of failure and the lockstepped CPUs provide zero switchover time. The FT server's modular design and remote management features allow for easy maintenance, and the in-the-box redundancy described earlier yields 99.999% availability (i.e. only five minutes of downtime per year)—a notable improvement over clusters, which offer only 99.99% availability (translating to over eight hours of downtime per year). Software costs are reduced because an FT server requires only one copy of the OS (Microsoft Windows 2000 Advanced Server, Microsoft Windows 2003 Enterprise Edition) and one copy of each application, unlike a cluster—thus providing all of the same benefits of a cluster, but with a lower total cost of ownership.

The other element of the hardware configuration is S1300 storage. Like the FT server, this fibre channel unit offers complete in-the-box redundancy, including dual I/O paths, dual RAID and cache controllers, and dual power units and batteries, and total data protection. Each unit can capacitate up to four terabytes of data, meeting even the most demanding organization's capacity requirements.

## *Software*

To facilitate the synching, failover and failback functionality between sites, the Disaster Recovery (FT) Solution relies on NEC EXPRESSCLUSTER<sup>®</sup> Software—the only software on the market that seamlessly integrates with and capitalizes on the internally redundant configuration of the FT server. This software is the component that allows transactions to be written to the servers at both sites simultaneously, making it possible to restore access to data instantaneously. The software also allows the system to fail over from one site to another when needed, and allows the system to re-synch automatically after a downed site is back online. EXPRESSCLUSTER is able to differentiate between a "disaster" (i.e. a hardware problem that requires failing over from one site to the other) and minor hardware issues that can be handled by the internal redundancy of an FT server and/or S1300 storage. This solution is unique because no other software is capable of recognizing this distinction, nor is capable of clustering over distances of up to a few hundred miles.

### *Service and Training*

The third important element of the Disaster Recovery (FT) Solution is service. Complete set-up and configuration service is available through highly trained, certified technicians, as is on-site training for IT staff in all pertinent maintenance and recovery procedures. Varying levels of ongoing technical support are also available, and can be tailored to the specific requirements of any organization.

### **Summary/Conclusion**

NEC is the first provider in the U.S. to implement a fully tested, fully certified, fault-tolerant disaster recovery solution that allows data to be written simultaneously to two locations across a WAN—providing total security for both applications and data. This solution retains all the benefits, but none of the drawbacks, of the alternatives, making it the only solution available today that offers 99.999% availability, automatic failover in case of disaster, disaster recovery within minutes, total transaction integrity despite disaster, and complete installation, configuration and support services—all at an affordable price. And its availability in two configurations—one for companies with users at two locations, and one for those with users at only one—means that there is a solution that is perfect for any organization.

### **About NEC Solutions America**

NEC Solutions (America), Inc. is a premier provider of integrated solutions for the Connected Enterprise in North America. As an affiliate of NEC Corporation (NASDAQ: NIPNY) (FTSE: 6701q.1), NEC Solutions America taps into a global resource network to help clients leverage technology to achieve a competitive edge. From mobile enterprise computing systems, biometric security solutions, business intelligence, projector and plasma display solutions, business services management and IT professional services, the expertise is delivered with the personal attention needed to address individual situations. With headquarters in Rancho Cordova, California, NEC Solutions America maintains research, marketing, sales and support facilities throughout the United States. Information regarding NEC Solutions America can be found at [www.necsam.com](http://www.necsam.com).

Information in this document is subject to change without notice. NEC and EXPRESSCLUSTER are registered trademarks and Empowered by Innovation a trademark of NEC Corporation and/or one or more of its subsidiaries. All are used under license. Microsoft, Windows, and Exchange are registered trademarks of Microsoft Corporation. All other trademarks and registered trademarks are the property of their respective owners. © 2004 NEC Solutions (America), Inc. All rights reserved.

NEC Solutions (America), Inc.  
2890 Scott Boulevard  
Santa Clara, CA 95050  
[www.necsam.com](http://www.necsam.com)