HITACHI
DATA SYSTEMS

Enterprise Storage

Improving Business Resilience with Data Replication and Storage Area Network Extension Technology

Business Continuity Solutions from Hitachi Data Systems and Cisco Systems, Inc.

A Solutions Summary

By Angela Magill and Christophe Bertrand of Hitachi Data Systems and Fabrizio Corno and Mark Allen of Cisco Systems, Inc.

July 2006

Executive Summary

With the cost of downtime routinely measured in millions of dollars per hour, and considering the wide-ranging legal, financial, and competitive fallout from even a minor outage to essential IT systems, regulators, investors, and insurers are paying closer attention to data protection and raising the priority of business continuity planning. Organizations large and small are now demanding greater resilience from the enterprise IT infrastructure.

Resilience is fundamental to any comprehensive business continuity strategy, and redundancy is one of the most effective ways of creating resilience. By duplicating critical components of the IT infrastructure, the risk of an outage from a single point of failure is substantially reduced. The irreplaceable data assets of an organization represent one of the most critical single points of failure in the infrastructure. Duplicating these critical assets, by maintaining constantly updated copies at a location a safe distance from the primary data center, safeguards data against loss and allows fast recovery from interruptions to the IT infrastructure.

The safe replication of data assets between geographically dispersed data centers is possible because of continual improvement in the speed and throughput of long-distance networks. Business continuity solutions that were once reserved for large organizations with dedicated dark fiber networks are now available to a much wider audience. Together, technologies that provide sophisticated replication, storage area network (SAN) extension, and high-speed long-distance IP networks are effecting a fundamental change in the level of protection given to critical enterprise data assets.

Hitachi Data Systems and Cisco Systems, Inc., are known individually for delivering high-availability solutions that support unparalleled business continuity. With unique capabilities and technologies, each company has made resilience of enterprise IT infrastructures a strategic imperative. Collectively, Hitachi Data Systems and Cisco offer the technology to effectively replicate application data across long-distance multiprotocol storage networks. Safeguarding these critical enterprise assets enables continuous business operations and speeds the recovery of applications in the event of a failure.

Hitachi Data Systems replication solutions support a wide variety of implementation scenarios, including combinations of local and long-distance replication using synchronous and asynchronous techniques. Cisco is uniquely positioned to provide fast and effective any-to-any connectivity across the globally dispersed networks of today's wired enterprise. Together, Hitachi Data Systems and Cisco provide a simplified, streamlined, and consolidated high-availability architecture to guarantee enterprise-wide business continuity.

Contents

Improving Business Resilience with Data Replication and Storage Area Network Extension Technology

Business Continuity Solutions from Hitachi Data Systems and Cisco Systems, Inc.

A Solutions Summary

By Angela Magill and Christophe Bertrand of Hitachi Data Systems and Fabrizio Corno and Mark Allen of Cisco Systems, Inc.

The Business Resilience Trend

The cost of downtime is staggering. On average, organizations lose US$1 million per hour due to system outages. And for those businesses highly dependent on IT, such as retail brokerages, losses can reach US$6.45 million per hour[1].

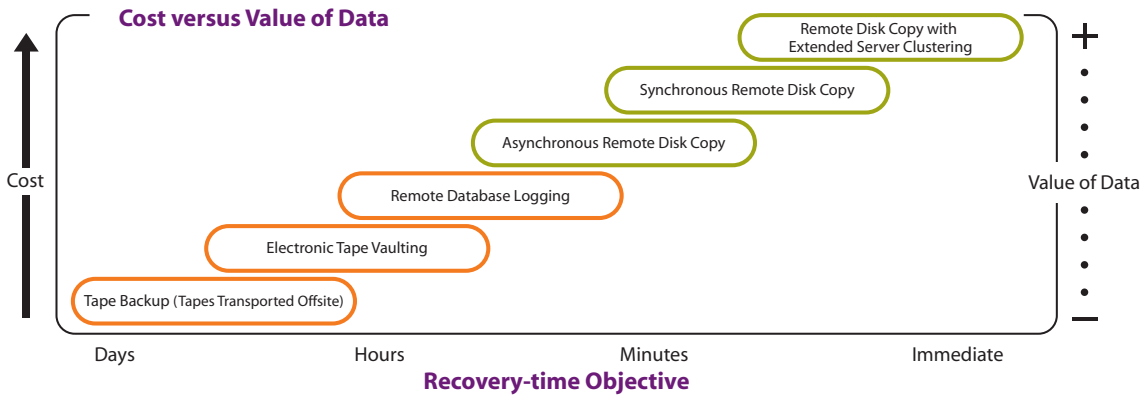
As if financial losses were not enough, studies by Binomial International reveal that 50 percent of companies that lose critical business systems for more than 10 days never recover. In today's highly competitive, 24/7 world of just-in-time delivery, global supply chains, and around-the-clock customer demand, an interruption to IT operations and the loss of critical business data have the potential to dramatically impact financial performance, competitive advantage, and business survival.

An organization's ability to weather unexpected outages without suffering catastrophic loss is receiving greater attention from insurers, investors, and government regulators. Many organizations now face legal oversight dictating mandatory levels of protection against data loss. In the United States the Health Insurance Portability and Accountability Act (HIPAA), Securities and Exchange Commission (SEC) rule 17a-4, Sarbanes-Oxley Act, Federal Drug Administration Code of Federal Regulations title 21 part 11, and Department of Defense (DoD) Directive 5015.2 "Records Management Program," are just some of the regulations providing guidance on electronic records retention and protection. The story is similar elsewhere in the world, with the New Basel Capital Accord (Basel II) affecting global corporations, RIPA and FAS in the U.K. and COB in France.

These regulations reflect growing concern in the business community for the survivability of electronic data following a catastrophic loss of IT services. Planning for business continuity in the event of unforeseen disaster is now considered a cost of doing business for organizations large and small. The surest way to guarantee the fast restart of critical business operations after an unexpected interruption is to build resilience into the IT infrastructure.

[1] Meta Group (recently acquired by Gartner)

Figure 1. Comparing Data Cost with Data Value.



Application recovery-time objectives and recovery-point objectives dictate the cost of data protection.

Assessing Risk

How far an organization must go to safeguard the IT infrastructure from failure is an assessment that must be made on a case-by-case basis. For applications that are critical to ongoing business operations, and where the risk of an outage is measurable, assessment is relatively straightforward. For example, if the data center hosting an online trading application is located in a flood zone, it is possible to calculate the probability of an outage and the annualized expected loss from the disruption. With this information in hand, a return on investment analysis can determine whether the cost of a business continuity solution is worth mitigating the expected losses. This type of rational risk management approach is essential when determining how to allocate limited IT resources to secure business continuity.

Data Replication Architectures

The most critical business applications invariably have the highest loss potential: the hourly cost of application downtime to the organization. For users of these applications, data replication can offer the fastest and most secure means of resuming operations after an outage.

During the data replication process, application write I/Os to a source storage system are duplicated and transmitted across a network to a second storage system. Depending on the type of replication chosen, the two storage systems remain perfectly synchronized, via synchronous replication, or closely synchronized, via asynchronous replication.

Replication techniques can be used both inside the data center, to address localized application interruptions, and between primary and remote data centers separated by thousands of miles, to provide extended protection from regional catastrophic events.

In-system Replication

Local, in-system replication provides a valuable complementary layer to a business continuity configuration. In-system replication offers a consistent point-in-time (PiT) copy of an entire system, a database, or a related set of volumes on a local storage system. This local backup is available for restore in case of a failure to the primary data, and it can optionally be used as a source for remote replication tasks.

Remote Data Replication

Remote replication of data to a secondary site, geographically separated from the primary data center, represents the most effective insurance policy against system downtime. Recovery from remotely replicated data is fast and substantially reduces the risk of data loss. As an added bonus, remote replication also provides for parallel access to business data, allowing read-only application workloads at the remote site to run without affecting regular production operations.

In addition to providing fast, automated failover during unplanned outages, replication technologies can reduce the application impact of planned downtime. Every data center requires periodic outages for system maintenance, testing, and backups. These activities can be disruptive to applications with round-the-clock service needs. Replication technologies support the seamless cut-over of operations to duplicate copies of production data, allowing primary system maintenance to proceed without affecting end-user application access.

Synchronous and Asynchronous Replication

There are two basic data replication techniques: synchronous and asynchronous. Each method provides different capabilities to suit the needs of a particular business continuity scenario.

Synchronous techniques treat application I/O at the local storage system and replicated writes to the remote copy as one process. The business application waits until both I/Os have completed successfully before proceeding. An incomplete operation at either location is rolled back in both places, guaranteeing that the remote copy is always an exact image of the primary.

Because synchronous replication keeps the two copies of data perfectly synchronized, integrity is guaranteed. This allows very fast application recovery after a disruption. Business operations interrupted by the outage can resume processing at the exact point the primary site stopped functioning.

The main drawback to synchronous replication is the impact of network latency on business application performance. In a synchronous replication configuration, the business application waits until both local and remote I/Os are complete before continuing. This means that any latency in the network between the local and remote copies of data directly affects application response time.

Asynchronous replication removes network latency from the application-performance equation. During an asynchronous replication process, a local write I/O is mirrored to the remote location, but the two writes are independent. After the local I/O is complete, the business application is free to continue processing, without waiting to receive acknowledgment of a successful remote write.

The decoupling of the local and remote I/Os allows asynchronous replication tasks to span unlimited distances without impacting application performance. Remote sites can be hundreds, or even thousands, of miles from the primary site, ensuring critical data is stored safely outside a disaster zone.

The downside to asynchronous replication techniques is the potential for I/O inconsistency between the source and target of the copy process. The slight time delay between local and remote writes means that in-flight transactions may be lost during an outage. This can lead to differences between local and remote copies of data. For replication technologies that enforce write-sequence fidelity, missing in-flight transactions raise the risk of data loss, but they do not compromise data integrity. However, if a replication solution cannot maintain the order of write I/Os—for example, if it relies on disk track updates—data integrity problems after a disaster can significantly increase application recovery time.

Write-sequence Fidelity and the Rolling Disaster

Database and file management applications use complex internal data structures to maintain integrity. Application write I/Os are processed in a precise order, reflecting internal dependencies in the software. To successfully recover these applications after a failure, replication solutions must adhere to the original sequence of write I/Os. Interfering with this sequence can introduce data integrity problems after a recovery.

The unexpected and chaotic nature of a disaster rarely provides a smooth cutoff between systems failing and initiation of the disaster recovery plan. The term Rolling Disaster describes a real-world effect, where systems, storage, and network connections fail at different times, spanning several minutes or hours. In this scenario, a system may be able to process transactions and issue updates to primary storage devices, but, due to earlier failures, updates may not propagate to a remote recovery site. Rolling disasters pose a significant challenge for applications that depend on write-sequence fidelity. Missing and out-of-sequence I/O at the remote location can result in corrupted and unusable data, requiring complex, time-consuming, and risky recovery processing.

Although the tight connection between local and remote write I/Os in a synchronous replication configuration precludes write-sequence errors, asynchronous configurations are not so fortunate. To avoid the consequences of a rolling disaster, an asynchronous replication solution must use caching, sequence numbering, time stamps, and other techniques to automatically preserve write-sequence fidelity at the remote site.

The Network

The network connecting local and remote storage systems is an often overlooked, but no less essential, component of a long-distance data replication configuration. The distance between the two storage systems often determines the type of data replication infrastructure. In a synchronous replication configuration, delays propagating updates to the secondary site affect local I/O response times. Depending on the business application's sensitivity to I/O performance, and the communications technology connecting the local and remote sites, the effectiveness of synchronous replication can begin to degrade at 20 miles to 100 miles (32km to 160km). This may not be far enough to safely clear a wide-area disaster zone.

Although Fibre Channel is the protocol of choice for enterprise storage area network (SAN) connectivity, mainframe environments that use host-based replication solutions are likely to require IBM® Enterprise Systems Connection (ESCON®) or Fiber Connection (FICON®) to connect local and remote data centers.

ESCON

ESCON is a 200Mbit/sec unidirectional serial bit transmission protocol for dynamically connecting IBM and IBM-compatible mainframes with various control units, including storage systems, tape drives and libraries, and network extension devices. ESCON provides nonblocking access through either point-to-point connections or high-speed switches called ESCON directors. Distance restrictions limit ESCON connectivity to less than 5 miles (8km), making it unsuitable for replication beyond local campus environments.

FICON

FICON is a 1.0625Gbit/sec or 2.125Gbit/sec bidirectional channel protocol, and the next-generation successor to ESCON. FICON, running over Fibre Channel, connects mainframes directly with control units or ESCON aggregation switches—and ESCON directors with a bridge card. The main advantage of FICON is support for extended distances between network nodes. FICON can reach a distance of 62 miles (100km) before experiencing any significant drop in data throughput.

Fibre Channel

Fibre Channel is a layered network protocol suite developed by ANSI and the favored protocol for open systems SAN connectivity. The protocol supports data transfers at 1.0625Gbit/sec, 2.125Gbit/sec, and 4.25Gbit/sec. Although distances vary with the type of cable deployed—single-mode (SM) or multimode (MM)—an SM fiber connection using long-wave (LW) optics can span about 6.2 miles (10km).

The Fibre Channel protocol uses a system of high-speed buffers, managed by the exchange of buffer-to-buffer credits, as a flow-control mechanism. In general, using full-size Fibre Channel frames (2148 bytes), a 1Gbit/sec connection requires one buffer-to-buffer credit for every 1.2 miles (2km). If bandwidth is increased to 2Gbit/sec, one buffer-to-buffer credit is only sufficient for 0.6 miles (1km). The throttling mechanism prevents buffer overruns, which can cause frames to be dropped. However, because storage systems typically carry a limited number of high-speed buffers—fewer than 10—the distance between two ends of a Fiber Channel network is restricted.

SAN Extension Technology

For business continuity planning purposes, the aim of replication technology is to provide a redundant copy of data far enough away from the primary storage system that it will not be impacted by a regional disaster. The restrictions of the ESCON, FICON, and Fibre Channel protocols limit the distance between local and remote data centers, presenting a barrier to long-distance data replication. SAN extension technology uses a variety of mechanisms to increase the distance between two end-points in a storage network. Designed into hardware components of the network, SAN extension technology optimizes the round-trip traffic between a local and remote data center, uses compression to reduce bandwidth consumption, and performs network protocol optimizations. These optimizations may include, for example, providing additional inline buffer credits to extend the reach of a Fibre Channel SAN, without reducing the line rate.

An Overview of SAN Extension Connectivity

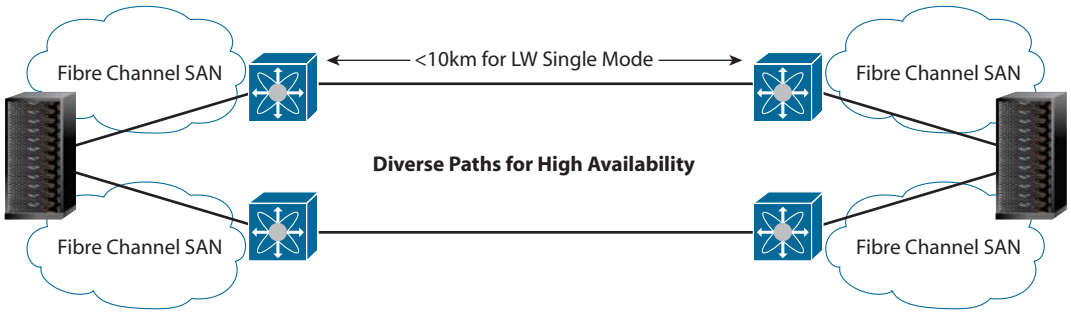
When evaluating SAN extension options for long-distance data replication, preexisting enterprise network infrastructure and service providers must be taken into consideration. In many instances, existing equipment—Fibre Channel switches, channel extenders, IP routers, SONET/SDH—can influence the final technology decision.

Dark Fiber

An organization with direct access to dark fiber has several options for extending SAN connectivity. For the simplest and easiest to manage approach, Fibre Channel can be flowed directly over the dark fiber infrastructure, eliminating the need for additional media and transmission conversion equipment.

The distance covered by a Fibre Channel over dark fiber network depends on the type of fiber deployed and whether any buffer-to-buffer credits are introduced to extend the connection. Using SM fiber with LW optics and no additional SAN extension equipment, a native Fibre Channel protocol connection can reach 6.2 miles (10km). MM fiber is not able to reach as far as SM, but it can provide a more cost-effective solution. The straightforward nature of a native Fiber Channel and dark fiber solution makes it fast to deploy, with low capital and operating costs.

Figure 2. Multilayer Fabric Switches Directly Connected by Diverse, Single-mode Dark Fiber Paths.



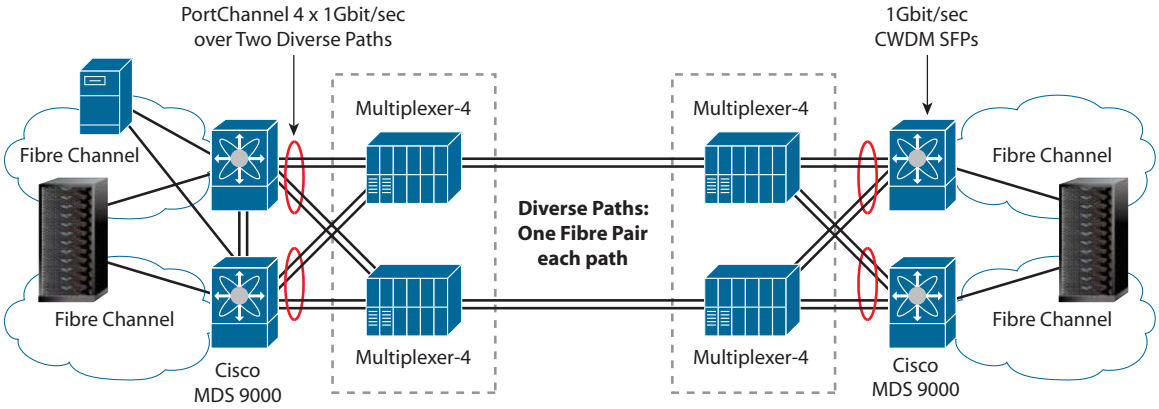
For the simplest and easiest to manage approach, Fibre Channel can be flowed directly over the dark fiber infrastructure, eliminating the need for additional media and transmission conversion equipment.

Adding wave division multiplexing technology to a dark fiber infrastructure increases the reach of an extended network and provides more bandwidth. Using Small Form Factor Pluggable (SFP) transceivers, existing dark fiber equipment can carry Coarse Wavelength Division Multiplexing (CWDM) signals to increase the distance between network endpoints on a single-mode fiber connection to 56 miles (90km).

Coarse Wavelength Division Multiplexing (CWDM)

CWDM is available in point-to-point or multiplexed configurations. In a multiplexed solution, SFPs are combined with Optical Add/Drop Multiplexer filters at each end of the network. The filters multiplex and demultiplex multiple CWDM wavelengths over the dark fiber connection, allowing the network to provide up to eight channels of traffic over a single fiber pair. Each of these channels can carry 1Gbit/sec or 2Gbit/sec Fibre Channel, 1Gbit/sec or 2Gbit/sec FICON, or 1Gbit/sec Ethernet for SAN communications.

Figure 3. CWDM Filter Solution Using Single-mode Dark Fiber Paths.



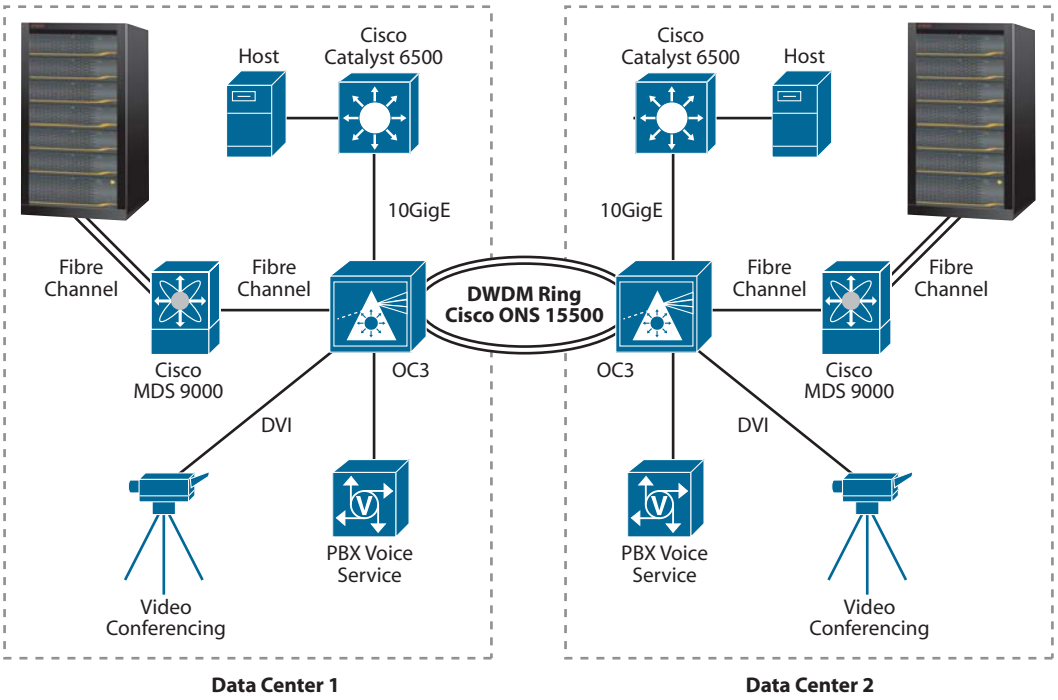
Filters multiplex and demultiplex multiple CWDM wavelengths over the dark fiber connection, allowing the network to provide up to eight channels of traffic over a single fiber pair. .

The multiple channels of a CWDM network increase available bandwidth and can host mixed SAN and Ethernet traffic, allowing an organization to optimize use of the dark fiber infrastructure. However, because OADM filters must be inserted at either end of the network, attenuation reduces the distance between end points to 41 miles (66km).

Dense Wavelength Division Multiplexing (DWDM)

Like CWDM, DWDM uses different optical frequencies to allow multiple channels of communication to travel simultaneously across a dark fiber infrastructure. However, with much greater precision in the division of optical wavelengths, DWDM is able to provide a massive increase in bandwidth compared to CWDM.

Figure 4. DWDM Solutions.



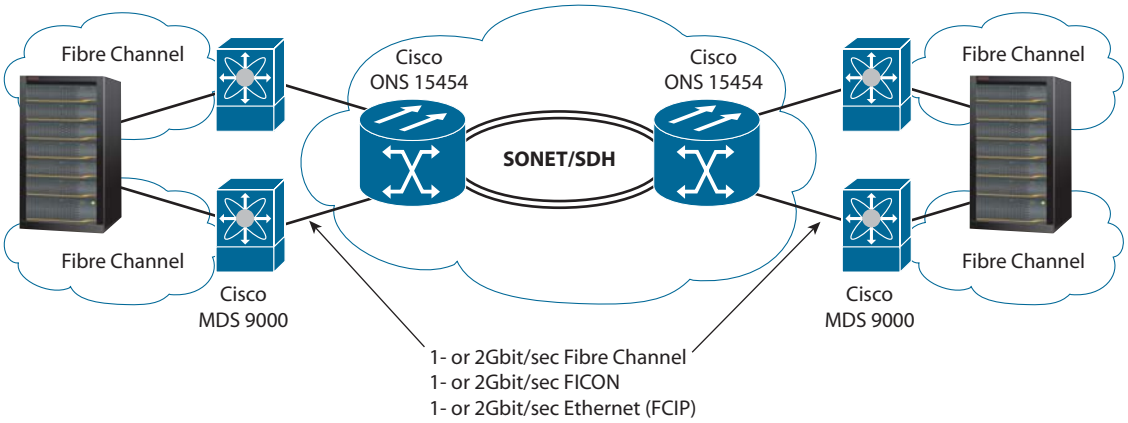
DWDM solutions support high-density service aggregation of storage and data networks.

DWDM solutions are capable of providing 32 channels of communication across a dark fiber network, delivering 320Gbit/sec of aggregated bandwidth. This high-speed, low-latency connectivity is ideal for extending mission-critical storage networks. DWDM solutions support the efficient aggregation of a diverse range of network protocols, including Fibre Channel, FICON, and ESCON storage networks, and Gigabit Ethernet (GigE), 10GigE, voice, and video data networks.

SONET/SDH

The synchronous optical network (SONET) and synchronous digital hierarchy (SDH) standards have been used to deploy high-speed communications networks for over 20 years. This well-known and trusted technology has evolved and now incorporates Ethernet and DWDM, giving enterprises and service providers fast, high-bandwidth communications. Widely deployed SONET/SDH networks have demonstrated their ability to meet the constantly changing needs of the enterprise. With guaranteed performance and quality of service (QoS), these networks are well suited to providing the backbone for SAN extension.

Figure 5. Fibre Channel over SONET/SDH.



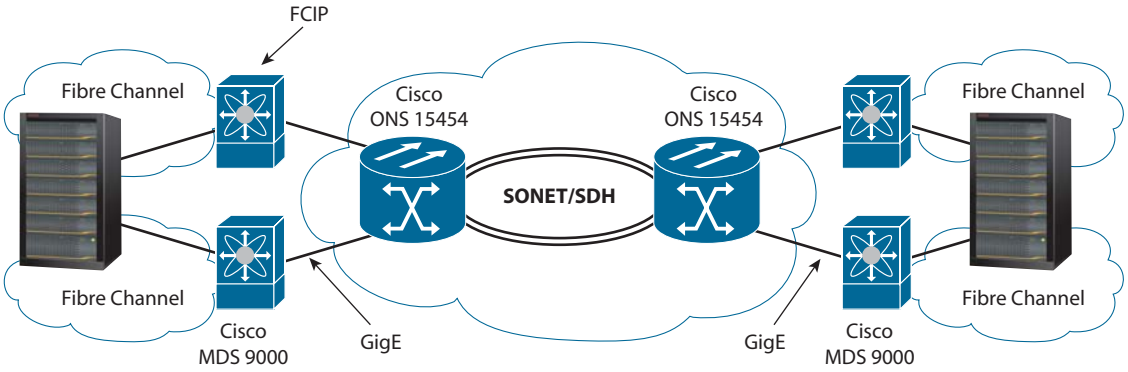
Enabling fast, high-bandwidth communications, SONET/SDH networks have demonstrated their ability to meet the constantly changing needs of the enterprise and are well suited to providing the backbone for SAN extension.

Fibre Channel over SONET/SDH processing introduces a delay of 20-25 microseconds at each transmission node. Each additional intermediate through-node introduces another 10-microsecond delay. The maximum allowable delay for synchronous replication tasks is generally considered to be 1 millisecond—500 microseconds each way. Considering that fiber propagation introduces an approximate 5 microsecond delay for each 0.6 miles (1km) traveled, the aggregate delay of processing Fibre Channel over SONET/SDH can quickly add up, limiting the distance between the source and target of a replication process to around 100km. The one benefit of SONET/SDH over upper layer transport methods, such as Fibre Channel over IP (FCIP) is that the delays are predictable.

Fibre Channel over IP (FCIP)

The FCIP protocol was developed by the Internet Engineering Task Force (IETF) to allow the transparent tunneling of Fibre Channel frames over an IP network. In an FCIP configuration, a gateway attached to a Fibre Channel switch transforms Fibre Channel frames from the SAN into IP frames and then sends these packets across an IP network. At the other end of the path a similar gateway receives the FCIP traffic and reverses the transformation, putting the packets on the remote Fibre Channel SAN. Using FCIP gateways, local and remote SANs can be connected to create a single extended Fibre Channel fabric.

Figure 6. Direct FCIP over SONET/SDH.



In an FCIP configuration, a gateway attached to a Fibre Channel switch transforms Fibre Channel frames from the SAN into IP frames and then sends these packets across an IP network.

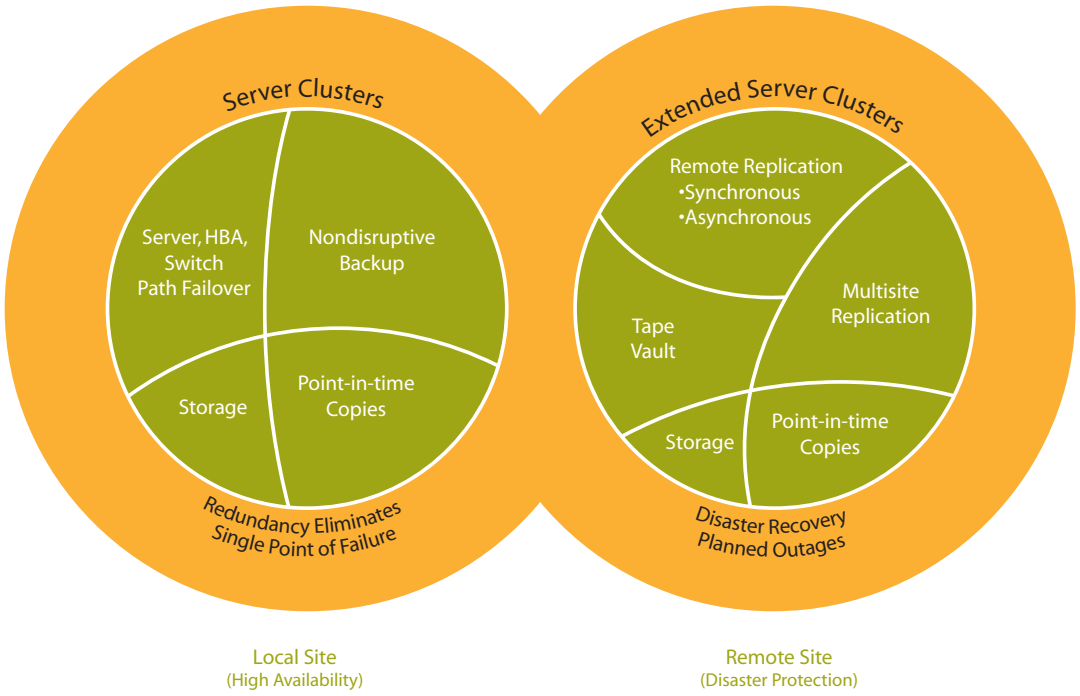
Because FCIP communications travel across TCP/IP networks, the distance between the source and target of a replication configuration is almost unlimited. But, as with any long-distance communication, the further apart the end points in the network the greater the potential for network latency to impact performance. The IETF has addressed some performance concerns with extended TCP options, such as enabling the TCP window size to scale to 1 gigabyte (1GB) to support greater sustained bandwidth rates. Theoretically, these new options would enable a 32 megabytes (32MB) TCP window with a 1Gbit/sec bandwidth to extend FCIP communications over 31,069 miles (50,000km) with 256 milliseconds of latency.

FCIP is fast and cost-effective to deploy because it leverages preexisting IP network infrastructures. Router-based IP services, like compression and encryption, apply equally to FCIP and data traffic. For organizations that do not manage their own transport infrastructure, FCIP offers enormous flexibility, as there is no need to switch between storage and data traffic.

Hitachi Data Systems Replication Solutions

Combining SAN extension technology and high-performance data replication greatly increases the business continuity preparedness of an organization. The innovative, storage-based replication solutions from Hitachi Data Systems offer long-distance data copy functionality between heterogeneous storage systems, satisfying a wide range of business continuity needs.

Figure 7. Hitachi Data Systems Business Continuity Framework.



The Hitachi Data Systems business continuity framework provides centralized, automated, policy-based management.

Hitachi TrueCopy™ Heterogeneous Remote Replication software bundle supports synchronous and asynchronous replication between Hitachi storage systems, and between any third-party storage systems virtualized behind the Hitachi TagmaStore® Universal Storage Platform or Network Storage Controller. TrueCopy Heterogeneous Remote Replication software offers administrators the flexibility to tune local and remote storage systems independently. This means that the source and target volumes of a replication process do not have to be of the same type or RAID configuration. For example, primary volumes in the main data center can be high-speed Fibre Channel devices with a RAID configuration tuned for performance, and secondary volumes at the remote data center can be cost-effective storage with RAID optimized for efficient use of capacity. Combining heterogeneous system support and configuration flexibility significantly alters the economics of business continuity, allowing an organization to protect more data at a lower cost.

TrueCopy software performs replication at the storage system controller, eliminating processing overhead on the host server and substantially reducing the impact of replication on business applications. The controller-based approach also enables a single replication solution to simultaneously satisfy the business continuity needs of applications running on mainframe, UNIX, and Microsoft Windows servers.

During synchronous replication, TrueCopy software duplicates each local I/O to the remote site, ensuring both copies are perfectly synchronized. I/O at the local and remote site must complete successfully before the application is allowed to continue. This ensures complete integrity of the replicated data during a failure.

Using a combination of techniques, which include sequence numbers and time stamps, TrueCopy software is able to replicate asynchronously over any distance with guaranteed I/O consistency, even when in-flight transactions are lost during an outage. By maintaining write-sequence fidelity at all times, application recovery at the remote site is fast and has guaranteed data integrity.

In addition to TrueCopy software, Hitachi Data Systems also supports local replication with Hitachi ShadowImage™ Heterogeneous In-System Replication software bundle; server-based replication for mainframes with Hitachi Compatible Replication software for IBM® XRC®, a cross-licensed technology from IBM; and asynchronous long-distance heterogeneous replication with Hitachi Universal Replicator software.

Universal Replicator software is a powerful data management and recovery solution for replicating data between heterogeneous storage systems attached to the Universal Storage Platform or Network Storage Controller. Ideally suited to copying data to multiple remote data centers, high-performance Universal Replicator software uses advanced journaling and cache management techniques to minimize the affect of replication on local storage users.

Replication technologies from Hitachi Data Systems can be combined to provide innovative, high-performance, out-of-region business continuity solutions that replicate data across unlimited distances.

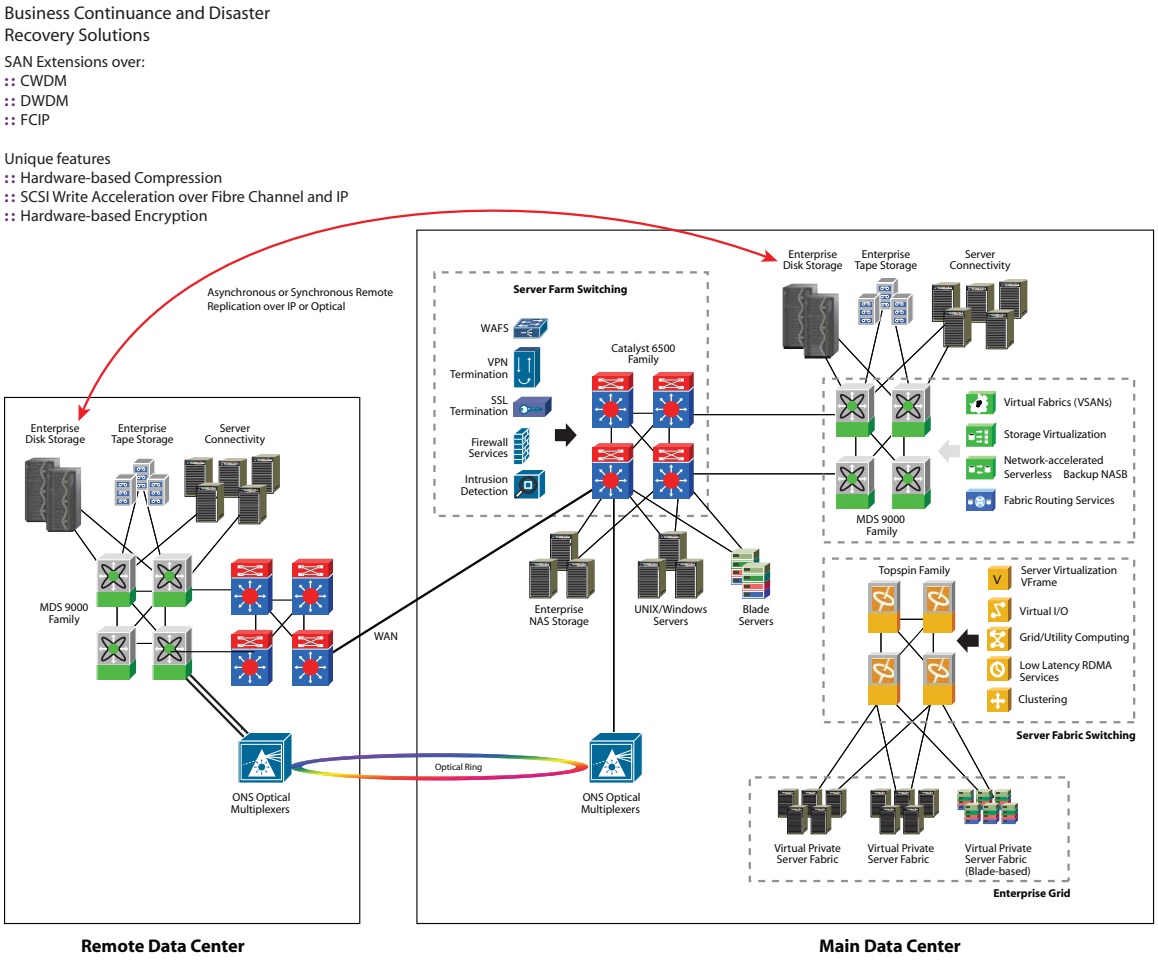
Cisco MDS 9000 Family SAN Extension Solutions

Complementing the replication solutions from Hitachi Data Systems, the Cisco MDS 9000 Family of fabric switches, directors, and intelligent software delivers best-in-class storage networking for business continuity. With integrated multiprotocol support for FCIP, the modular Cisco MDS 9200 Multilayer Fabric Switch series and the MDS 9500 Multilayer Director series help organizations leverage existing investments in IP networks and support hosting of SAN extension and local fabric switching services on a single platform.

The Cisco MDS 9000 IP Storage Services Module (IPS) and Cisco MDS 9000 Multiprotocol Storage Service Module (MPS) provide the technology to extend storage traffic over long-distance IP networks. Seamlessly integrated into the Cisco MDS 9000 Family directors and switches, the IPS, with 8 GigE ports, and the MPS, offering 14 Fibre Channel and 2 GigE ports, enable replication traffic originating on a Fibre Channel SAN to flow across an IP network connecting local and remote data centers.

The Cisco MDS 9000 switch and IPS provide a high-performance, highly available bridge between a local Fibre Channel SAN and the long-distance IP infrastructure. Support for network QoS and virtual SANs (VSANs) allows storage replication traffic to be effectively segregated and independently managed over a shared network infrastructure. The Cisco MDS 9216i and MPS offers up to 3500 additional buffer credits on a single Fibre Channel port, making native Fibre Channel extension a viable option for many applications. These modular solutions from Cisco provide support for a complete portfolio of optical transmission platforms, including CWDM, DWDM, and SONET/SDH, for native long-distance Fibre Channel and FCIP connectivity.

Figure 8. Local and Remote Data Centers with Cisco Business Continuity Solutions Deployed.



With integrated multiprotocol support for FCIP, the modular Cisco MDS 9200 Multilayer Fabric Switch series and the MDS 9500 Multilayer Director series help organizations leverage existing investments in IP networks and support hosting of SAN extension and local fabric switching services on a single platform.

Extending Virtual SANs

In many existing IT environments, backup solution design has involved building a separate, parallel storage network for backup traffic. From a technical and operational perspective, a separate storage network provides flexibility, security, and high availability for the backup infrastructure, albeit at a higher cost. While separate storage networks help guarantee performance and alleviate fabric-wide disruptions,

these solutions are also expensive, requiring separate switches and complicated additional management, and they often lead to the costly waste of ports.

Cisco delivers advanced technology revolutionizing storage network deployments using a VSAN capability. Included in the Cisco MDS 9000 SAN-OS software, VSANs allow a single physical SAN fabric or switch to support multiple, fully independent storage networks. Each VSAN is separately zoned, and supports its own fabric services for resilience and stability.

Cisco IPS and MPS supports the extension of VSANs across long-distance IP networks. In a replication configuration, this ability to effectively segregate multiple streams of traffic, each originating from a different SAN, optimizes the use of the long-distance network bandwidth and provides true end-to-end QoS. Combining the segregation of traffic with QoS support in the switch allows replication tasks with different priorities to effectively share the same extended SAN connectivity. For example, when replicating in a tiered storage environment, VSANs can ensure priority is given to top-tier business continuity traffic.

Although VSANs enforce segregation, Inter-VSAN Routing (IVR) provides a mechanism for traffic to transit VSAN boundaries. This adds flexibility without compromising the stability and availability of each VSAN.

Reducing SAN Complexity

The modular, single-chassis architecture of the Cisco MDS 9000 solutions eliminates the need for additional SAN extension devices in the network. Integrated support for multiple protocols eases management of Fibre Channel, FCIP, FICON, IP, and iSCSI connectivity. And, with a single solution providing local Fibre Channel and remote IP services, storage network complexity is reduced, giving administrators fewer platforms to manage.

The Cisco MDS 9000 solutions integrate easily into existing networks and are administered using standard Cisco management tools—Fabric Manager, CiscoWorks, CiscoView, Cisco Transport Manager, and Cisco SAN-OS® command-line interface. Network and storage administrators maintain secure, roles-based access to these management tools over an out-of-band Ethernet connection, a serial RJ-45 interface, or in-band over Fibre Channel connectivity. The use of common management tools boosts administrator productivity and reduces training and IT costs.

Improving Network Performance, Resilience, and Security

The Cisco MDS 9216i, MDS 9000 IPS, and MDS 9000 MPS support FCIP compression to optimize bandwidth, allowing data replication across low and intermediate bandwidth long-distance networks. Under optimal conditions, compression ratios of up to 30 to 1 are possible, with typical ratios of 2 to 1 for a wide variety of data types. The Cisco MDS 9216i and MPS can also perform real-time encryption of data, allowing replication traffic to be securely transported over public networks.

The FCIP write-acceleration feature significantly improves replication performance when traffic travels over extended IP distances. With FCIP write-acceleration enabled, the latency of each Fibre Channel command acknowledgement is substantially reduced. This optimizes overall network throughput.

The Cisco MDS 9000 SAN-OS software includes tools to monitor and optimize the performance of an FCIP connection. Storage administrators can use the SAN Extension Tuner software feature to fine tune the TCP/IP parameters used by FCIP over the IP network. This ability to adapt TCP/IP behavior to the specific network configuration in use can significantly improve performance.

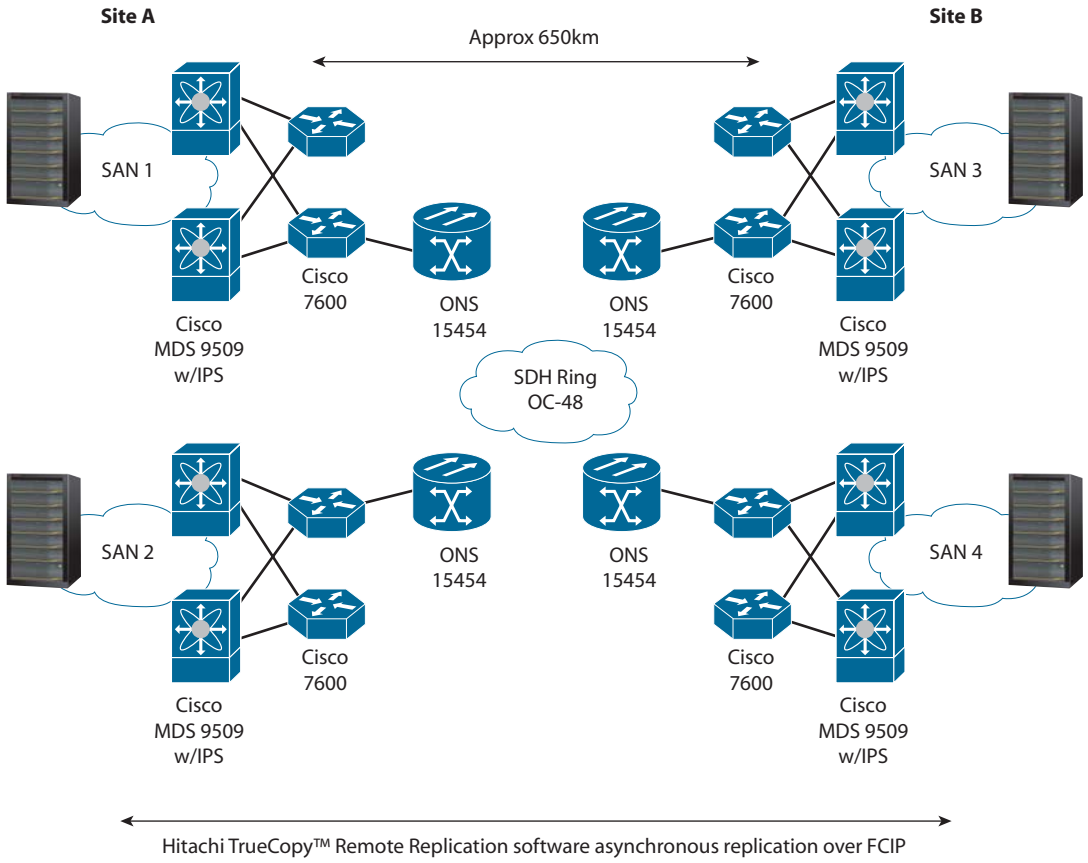
The Cisco MDS 9000 Family also supports the Virtual Router Redundancy Protocol (VRRP). This allows GigE interfaces to be grouped to give FCIP endpoints higher availability.

Replicating a Real-time Trading Application with FCIP

Recognizing the critical importance of business continuity planning, a leading financial services firm made the decision to replicate data from its real-time trading application, hosted at the primary data center, to a secondary storage system located at a remote site. By maintaining copies of data at a distant location, the firm was able to guarantee protection of data against loss from a regional catastrophe.

The remote site chosen for the replicated copy was separated from the primary data center by 650 miles. This raised the issue of how to effectively replicate data over such a long distance.

Figure 9. Long-distance Replication of Real-time Trading Application Data.



Hitachi Data Systems and Cisco implemented a joint solution that employed Hitachi TrueCopy™ Heterogeneous Remote Replication software bundle to asynchronously replicate the trading application data over an extended SAN using FCIP.

With existing infrastructure components in place, Hitachi Data Systems and Cisco were well placed to help the IT group with the long-distance data replication configuration. After performing a detailed risk assessment to determine business continuity requirements of the application, Hitachi Data Systems and Cisco implemented a joint solution that asynchronously replicated the trading application data over an

extended SAN using FCIP. With a SONET/DSH infrastructure already in place, the firm was able to quickly set up a fully redundant FCIP replication configuration to satisfy its business continuity needs.

A Combined Approach to Business Continuity

Effective long-distance data protection requires two fundamental components: replication technology and an extended storage network infrastructure. Together, the replication and SAN extension solutions from Hitachi Data Systems and Cisco provide a highly available architecture to guarantee access to data no matter what events befall the organization.

Supporting the transport of storage data over a wide range of networking infrastructures, the Cisco MDS 9000 Family of solutions provides any-to-any connectivity, configuration flexibility, and massive consolidation to satisfy the most demanding enterprise business continuity requirements. Complementing the Cisco infrastructure at the data layer, replication technologies from Hitachi Data Systems support a wide range of different configurations to guarantee data availability, speed application recovery, and minimize downtime to critical IT systems. Together, Hitachi Data Systems and Cisco deliver business continuity solutions that simplify and streamline the enterprise IT infrastructure, build high availability into the fabric of the enterprise, and maximize investment through massive economies of scale.

Hitachi Data Systems Corporation

Corporate Headquarters
750 Central Expressway
Santa Clara, California 95050-2627
U.S.A.
Phone: 1 408 970 1000
www.hds.com
info@hds.com

Asia Pacific and Americas
750 Central Expressway
Santa Clara, California 95050-2627
U.S.A.
Phone: 1 408 970 1000
info@hds.com

Europe Headquarters
Sefton Park
Stoke Poges
Buckinghamshire SL2 4HD
United Kingdom
Phone: + 44 (0)1753 618000
info.eu@hds.com

WHP-221-00 July 2006