BUSINESS CASE

THE JUSTIFICATION FOR BUSINESS CONTINUANCE

BENEFITS OF BUSINESS READY DATA CENTERS

- Protect—The Cisco Business Ready Data Center protects valuable resources and services with security and business continuance networking technologies, helping to ensure maximum application availability and regulatory compliance in the event of disruption.
- Optimize—The Cisco Business Ready Data Center optimizes user productivity and resource usage with an extensible architecture and proven integrated reference designs that reduce total cost of ownership (TCO), consolidate and simplify disparate systems, and increase productivity.
- Grow—Based on the Cisco Intelligent Information Network vision, the Cisco Business Ready Data Center supports growth with a scalable and adaptive architecture that facilitates business agility and speeds time to market.

EXECUTIVE SUMMARY

A robust business continuance strategy keeps essential services operational during and after a disaster or failure, and restores noncritical services before they adversely impact the organization. Fortunately, as the need for business continuance increases, the cost of associated technologies and solutions is falling. Still, the cost of business continuance can be significant; therefore, budget is a primary concern for those people developing business continuance strategies for their organizations.

Disruptions can destroy a business. Studies show that companies without business continuance plans are at higher risk of business failure than those with them. Gartner Group estimates that 43 percent of businesses fail within five years following a major disaster and 29 percent fail within the first two to four months. While network downtime and subsequent loss of productivity from the inability to access mission-critical applications in the data center can cost thousands, even millions, of dollars per hour, there can be long-term consequences even after systems are restored. Customers can lose confidence and go to a competitor. An organization can also suffer brand dilution and even litigation. Therefore, business continuance is of paramount importance for enterprises, and central to the plan is assuring continuous access to applications housed in the enterprise data center. Given an increasing need to conform to recent government legislation such as HIPAA, Sarbanes-Oxley, and SEC T+1, the implementation of an effective business continuance strategy has risen to the top of many CIO to-do lists.

For many organizations, effective business continuance implementations support the most *rapid recovery* for the *most critical business applications and data* in the *shortest time possible*. With this in mind, a logical approach is one that layers continuance support atop a newly consolidated data center and storage infrastructure. In a recent study, Gartner Group shows that over 90 percent of data centers will have completed some form of consolidation over the next few years.

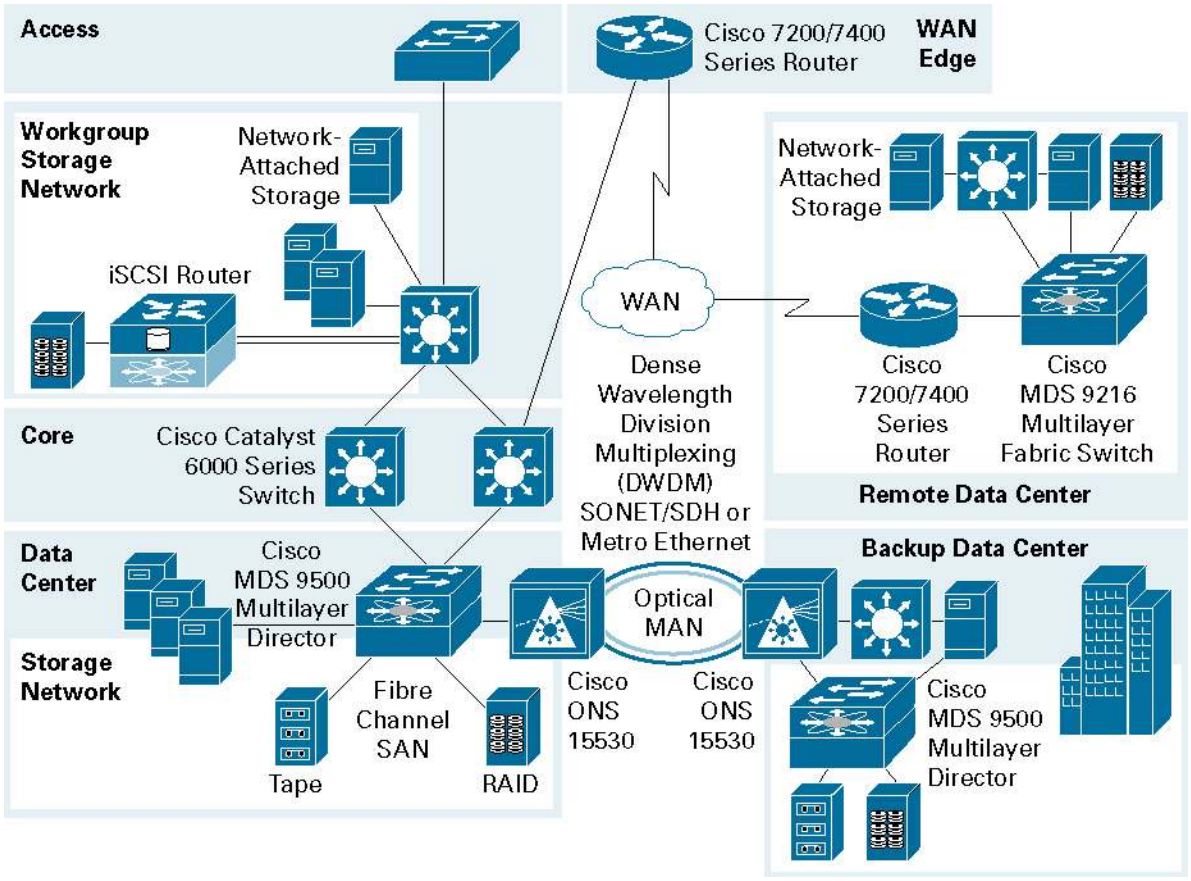
This business case demonstrates how Cisco® Business Ready Data Center solutions support an effective infrastructure for business continuance through a unique combination of advanced technology, cross-product integration, and management best practices. Results include payback periods of less than a year and implementation return on investment (ROI) ranging from 72 percent to over 1000 percent.

BUSINESS READY DATA CENTER—ENABLING BUSINESS CONTINUANCE AND DISASTER RECOVERY

Organizations require a business continuance strategy that protects data and ensures rapid system recovery. Any business continuance strategy depends upon a storage network that enables critical data replication and backup, rapid system recovery, and end-user access from any location. Deploying redundant data centers, then interconnecting them over distance, is a critical component of most viable business continuance plans (Figure 1).

Figure 1

Data Center Network for Disaster Recovery and Business Continuance



The Gartner Group recommends that the location of a secondary site for disaster recovery be far enough away from the primary data center to reduce the likelihood of all business-critical IT operations being affected by the same disaster. The storage network that connects these geographically dispersed sites should have high-performance, reliable, and secure communications, providing a critical foundation for allowing the business to continue operations even while recovering from a disaster.

There is no “one size fits all” solution for business continuance. Most companies require a portfolio of business continuance solutions to match application-specific factors such as recovery time objective, data loss criteria, technical feasibility, and business impact of associated cost. Cisco Systems® offers a portfolio of intelligent IP, storage, and optical networking solutions that provide the high-performance, reliable, secure infrastructure required for data protection and recovery strategies, such as data backup, replication, and mirroring across the local, metropolitan, and wide area. In addition to back-end solutions focused on data protection and recovery, Cisco also provides networking solutions that ensure continuous user access to applications and data.

The Cisco Business Ready Data Center product portfolio offers customers any combination of Enterprise Systems Connection (ESCON), Fibre Channel, IBM Fiber Connection (FICON), Internet Small Computer System Interface (iSCSI), and Fibre Channel over IP (FCIP) technologies to build or expand their storage-area networks (SANs). This portfolio includes the Cisco MDS 9000 Series Switches, the FCIP Port Adapter Interface for the Cisco 7200 and Cisco 7400 series routers, the Cisco SN 5400 Series Storage Router, and Cisco ONS 15000 series optical networking platforms.

THE CRITICAL MECHANISMS—REPLICATION AND MIRRORING

Traditionally, many business continuance plans rely upon creating backup tapes in-house, then physically transporting them offsite to a backup data center. To avoid the time delays, effort, expense, and security risk of physical transport, companies now use the efficiency, speed, and security of a high-performance network connection to one or more remote backup sites. In particular, the high-availability metropolitan-area network (metro or MAN) services based on dense wavelength-division multiplexing (DWDM), SONET/SDH, and the long-distance reach of FCIP and storage over SONET can reduce application and system recovery time from days to a few minutes, depending upon specific recovery techniques and the supporting infrastructure. Table 1 lists the more popular techniques and their associated time to recovery, data loss, distance, and cost tradeoffs.

Table 1. Business Continuance Approaches and Tradeoffs

	Time to Recovery	Amount of Data Loss	Distance	Costs
Tape Backup Onsite Tape		**High** Dependent on Backup Frequency (Risk All Data Being Lost if Not Transported Offsite)	**SAN/Campus**	Host $ Software $ Tape $$ Network $
Remote Electronic Vaulting	Hours–Days	**High** Dependent on Back up Frequency	**Metro/WAN**	
Replication Remote Asynchronous Replication	Hours	**Low–High** Dependent on Frequency of Replication and Available Bandwidth	**SAN/Campus/MAN/WAN**	Host $ Software $ Tape $$ Network $$$
Mirroring Synchronous Disk	Minutes–Hours	**Zero**	**SAN/Campus/MAN**	Host $ Software $$ Tape $$ Network $$
Data Center Mirroring	Immediate–Minutes	**Zero**	**SAN/Campus/MAN**	Host $$ Software $$ Tape $$ Network $$

For applications that require much faster recovery than can be expected from more conventional tape backup, and for applications that have little tolerance for data loss, IT organizations should consider data-replication and data-mirroring techniques, which provide significant advantages over tape backup. They enable maintenance of two sets of data at all times. For business continuance purposes, data sets are typically housed in separate locations, and maintained either synchronously or asynchronously. The following sections discuss the implementation of each approach within the context of a data-center network.

Remote Asynchronous Replication

Asynchronous replication is preferable when a backup site is located beyond the metro area because latency between sites would impact the performance of the production application. Asynchronous replication software uses network bandwidth efficiently by transferring only changed data blocks or tracks to a remote backup system. This technique requires much less bandwidth than transfer of full tape backups, and enables faster data recovery in case of data corruption or a major disruption at the production site. The development of new standard networking protocols such as FCIP reduces the cost of deployment by allowing SAN extension over IP networks rather than requiring more traditional dedicated leased lines. Alternatively, storage over SONET supports SAN extension.

To better meet application requirements, Cisco offers a number of flexible options for SAN extension. The IP Storage Services Module in the Cisco MDS 9000 Series supports FCIP, along with dedicated port adapters in Cisco 7400 and Cisco 7200 Series routers and in the Cisco SN 5428-2 Storage Router. FCIP can be transported over most IP WANs, SONET, or DWDM networks as user needs dictate. The Cisco ONS 15454 Multiservice Provisioning Platform (MSPP) provides storage-over-SONET capability in its SL Series interface, which supports Fibre Channel and FICON transport.

Synchronous Disk Replication and Mirroring

Synchronous disk replication or mirroring is ideal for applications that demand complete data integrity, requiring the fastest recovery and no transaction loss. These solutions synchronously replicate all disk writes to a backup storage system located at a remote site. Host-based synchronous mirroring is an alternative to storage-based synchronous replication. The host writes simultaneously to both the local SAN and to the remote disk. Both replication and mirroring require a low-latency, high-speed, highly reliable storage network because substantial latency can degrade application performance.

Many networking technologies are suitable for synchronous replication and mirroring. Where dark fiber is available, the Cisco ONS 15540 ESP Extended Services Platform, Cisco ONS 15530 DWDM Multiservice Aggregation Platform, or Cisco ONS 15454 Multiservice Transport Platform (MSTP) support DWDM transport of multiple high-speed channels of different types (for example, ESCON, Fibre Channel, and Gigabit Ethernet) across a single fiber pair. By supporting distances up to 600 kilometers (km) without reducing the bandwidth available to any channel, Cisco solutions for metro optical networks facilitate synchronous mirroring across a broad geographical area.

Data-Center Mirroring

For nearly instantaneous failover to a backup site, IT organizations can consider data-center mirroring, where both fully synchronized production and backup data centers share workloads. There are two ways to design data-center mirroring systems. In the first and more complex design, the same application is load balanced across two mirrored sites. Individual user sessions are directed to the most available site by an intelligent load-balancing system. In the second, more common design, each data center supports a different set of applications. When a failure occurs in one site, the surviving site takes over the affected applications.

The Cisco ONS 15454, Cisco ONS 15530, and the Cisco ONS 15540 platforms meet the latency and bandwidth requirements of data-center mirroring by creating a high-speed metro network. These platforms also support the multiple channels required for user access, system synchronization, and storage replication.

The following section discusses a new model for networked recovery and continuance that effectively and economically supports both storage replication and mirroring.

THE NEW NETWORKED RECOVERY AND CONTINUANCE MODEL

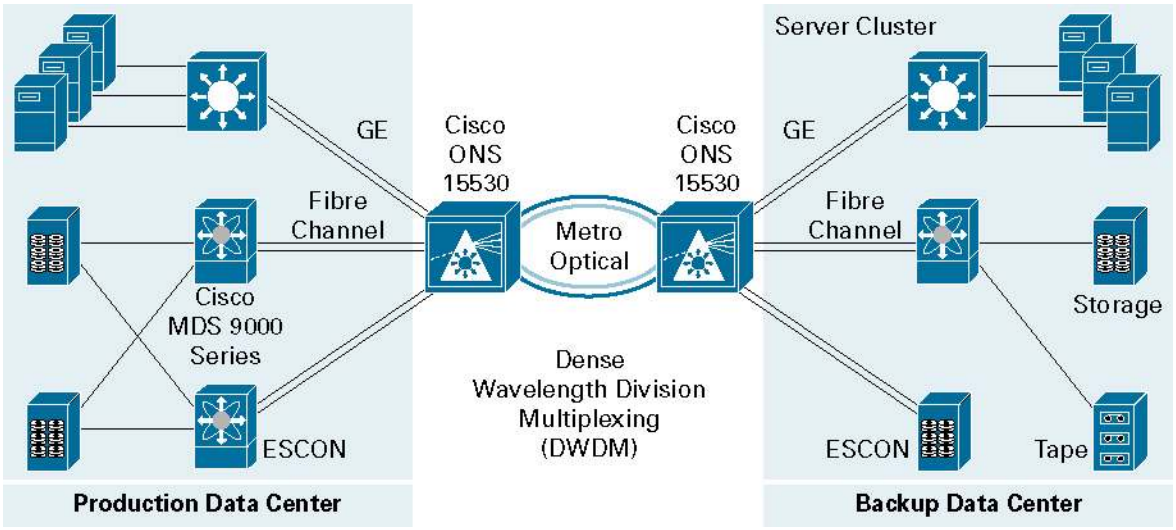
Traditional approaches to disaster recovery and business continuance resemble the early stages of networking technology. Similarities include extensive use of point-to-point connectivity, application-specific connections, and a close coupling between a specific connection and the data transported across that connection. For example, there are different approaches for supporting disaster recovery and business continuance for mainframes and Web-application systems. For mainframes, expensive connectivity is based upon wide-area ATM services, sometimes costing users nearly US$50,000 per month for ATM OC-3 services. The more cost-effective approach extends Fibre Channel over either SONET or DWDM.

Using circuit-oriented protocols such as ATM, Frame Relay, or point-to-point to transport data traffic through a metro network creates performance inefficiencies and needlessly increases network complexity. Often this is directly related to the need for protocol conversions in transitioning traffic from the Ethernet LANs to an ATM metro on both sides of the connection. Furthermore, these complexities outpace the skills of available IT talent. This situation makes it more difficult to hire, train, and retain the staff required to run multiprotocol networks. It also leads to cost increases, provisioning delays for new services, and more complex network operation and management.

Customer Example

Many users choose to implement an approach similar to that of a Cisco customer that was plagued by an inefficient disaster-recovery transport that became more expensive to support and maintain. This customer replaced its existing disaster-recovery infrastructure with a metro DWDM optical ring based on the next-generation Cisco ONS 15530 (Figure 2).

Figure 2
DWDM-Based Network Transport Aggregation



This customer implemented DWDM as the technology of choice for the following reasons:

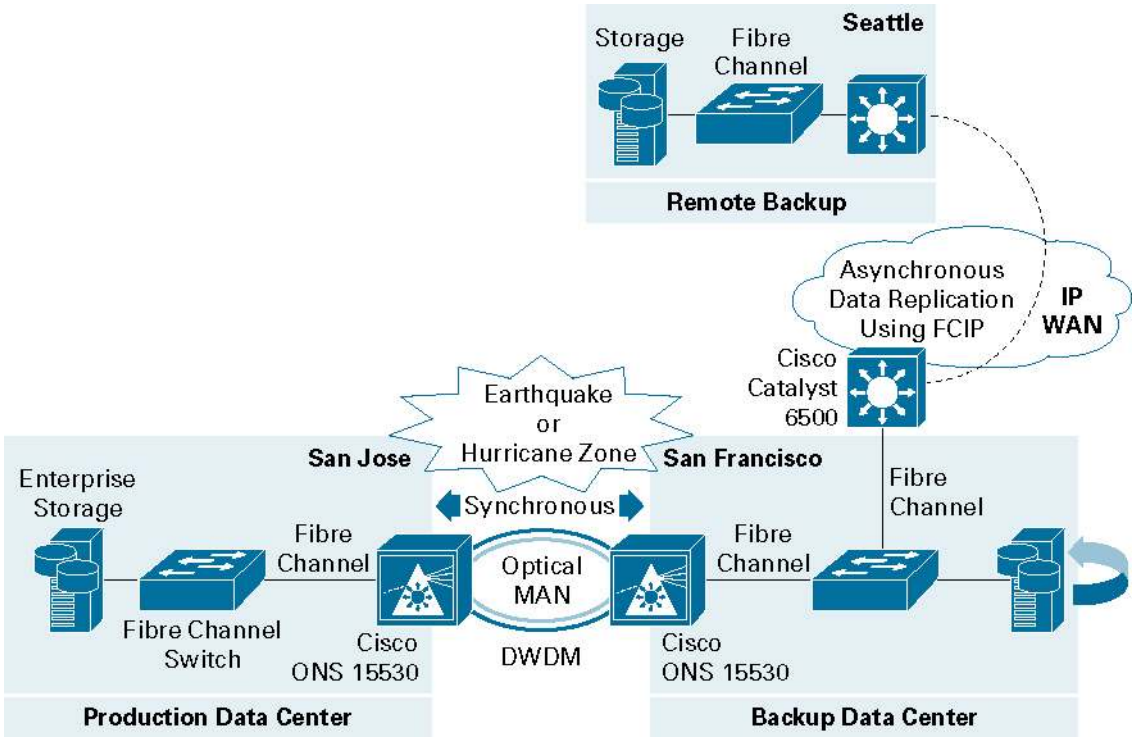
- Attractive return on investment—The customer reduced disaster-recovery total cost of ownership (TCO) compared to ATM by US$100,000 per year for the first five years. During the second five years, the fiber backbone network was already paid for, providing 320 Gbps of bandwidth free of charge. The business case was based on the company's decreased costs for WAN services and capital equipment purchase and maintenance.

- Improved application performance due to higher bandwidth and lower latency—Applications with disk-intensive input and output, especially writes, were less affected by the level of backup in place at any one time, enabling greater flexibility in implementing phased recovery improvements.
- Server clustering across metro for faster recovery and resource usage—Clustering, traditionally a distance-sensitive technology, could now be distributed across a larger area, improving the quality of nonstop business operation by limiting the impact of any application, system, or data-center outage.
- Flexibility to support future business and application requirements—DWDM indiscriminately supports upper-layer network protocols. Today, it supports Gigabit Ethernet, ESCON, and Fibre Channel equally well. These three protocols are all industry standards. DWDM transport can easily support other high-speed network standards as they become available.

On the basis of both business and technical criteria, the customer decided that a DWDM solution with the Cisco ONS 15530 platform met their existing requirements and would scale to meet future requirements. It allowed the customer to use EMC Symmetrix Remote Data Facility (SRDF) over Fibre Channel to improve synchronous-mirroring performance and throughput. The lower latency of DWDM also improved performance of end-user applications. This infrastructure allowed the customer to expand from a purely point-to-point topology to a multisite topology, achieving replication across multiple sites.

The customer can also extend the reach of its disaster recovery and business continuance to address the needs of other users beyond the metropolitan area, especially in places at high risk for earthquakes, hurricanes, or severe flooding, without compromising operational availability or recoverability (Figure 3). This model enables a cost-effective, second-tier backup mechanism through asynchronous data replication with FCIP as the primary transport mechanism over a lower-speed communications channel (between fractional T3 and fractional OC-3 rates).

Figure 3
Secondary Data Backup Approach Using FCIP



The next section discusses the quantitative business benefits associated with using a Cisco technology-based approach to support this collective capability.

BUSINESS CASE DETAILS

A highly effective approach for disaster recovery and business continuance supports the most rapid recovery for the most critical business applications and data in the shortest time possible. In many businesses, the optimal time for implementing this approach is upon completion of data center and/or storage consolidation. After consolidation, a greater mass of systems, applications, and data resides in fewer locations, thereby making it more effective and economical to implement business continuance.

This approach is an important guiding principle of this business case. This case study assumes completion of all related consolidation activity and that the objective of the continuance initiative is to facilitate highly available business operations as previously described.

THE COST OF DOWNTIME

The reference point for the cost of downtime in this business case is the data provided by a recent Infonetics study, "*The Cost of Enterprise Downtime, 2003*"[1]. The results provide useful insights into both the causes and impact of unplanned downtime. For all study participants, the total cost of downtime (including lost revenue and degraded productivity)[2] is less than one percent of total revenue, averaging between 0.2 and 0.3 percent (Table 2). Although seven downtime sources were analyzed in the research (transport network, security services, wiring, servers, applications, service providers, and e-commerce transactions), the three most significant sources of unplanned downtime are servers, the network, and applications, collectively accounting for 72 percent of all downtime. The revenues and costs in Table 2 are calculated in U.S. dollars.

Table 2. Downtime Cost as a Percentage of Revenue (Source: Infonetics)

Case Study	Annual Revenue	Downtime Hours	Downtime Cost	Percentage of Revenue	Cost per Hour
Energy	$6.75 billion	2648	$4.3 million	0.1%	$1624
High tech	$1.3 billion	2448	$10.2 million	0.8%	$4167
Healthcare	$44 billion	772	$74.6 million	0.2%	$96,632
Travel	$850 million	62	$2.4 million	0.3%	$38,710
Finance (United States)	$4.0 billion	374	$10.6 million	0.3%	$28,342
Finance (Europe)	$1.2 billion	241	$379,000	0.0%	$1573

[1] The study objective was to understand the causes and calculate the cost of outages and service degradations in terms of lost revenue and lost productivity at six major organizations of various industries. In order to provide the most specific and accurate information possible, the study focused upon seven potential causes of system and application downtime: network products, security, cables and connectors, servers, applications, service providers, and e-commerce.

One premise of this research was that end users generally would not be able to articulate the exact quantitative impact of downtime on their organizations. Instead, the research addressed questions that respondents could answer accurately: how often do they have outages and degradations attributable to each of the individual causes of downtime, how long do those outages and degradations last, and how many users are affected by those outages and degradations. Researchers then compiled the information from the completed questionnaires and calculated the resultant costs of downtime at each organization.

[2] Lost revenue accounts for 72 percent of the total cost of downtime with degraded productivity constituting the remaining 28 percent. The revenue specific data points for this business case were found in the Global 1000 listing, as compiled and reported by *Business Week*. Details of member companies and their associated revenues can be found at: http://bwnt.businessweek.com/global_1000/2003/index.asp

Using annual revenue ($3,470,000,000) for the 1000th member as a starting point, we take .1 percent of revenue ($3,470,000), the lower end of the Infonetics findings, as a highly conservative estimate of the worst case cost of downtime for Global 1000 companies. Given that the cost of downtime reflects both lost revenue and degraded productivity, we then multiplied the $3.47M revenue figure by 72 percent to focus upon lost revenue. This calculation gives us $2,411,650 as the actual lost revenue figure and the starting point for our solution benefit analysis.

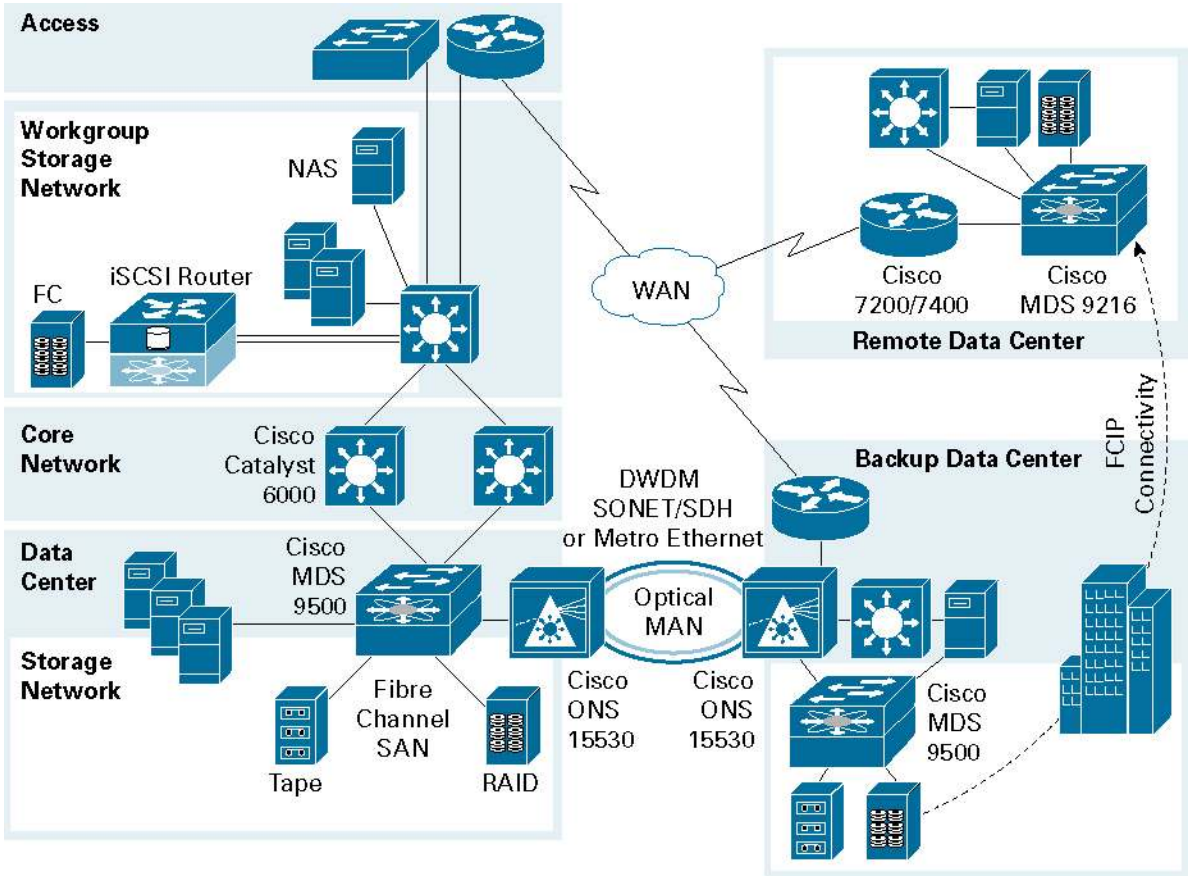
This business case assumes the prior completion of all relevant data-center consolidation activity. This assumption associates solution benefit with solution cost. In this case, the solution is independent of the storage-networking solution, requiring only IP, Fibre Channel, Gigabit Ethernet, and DWDM technologies.

SOLUTION PRICING

The primary solution components are the Cisco ONS 15530 DWDM MAP and a leased fiber network (Figure 4). Based upon estimated costs from AT&T, Table 3 lists capital and network-specific facilities costs.

Figure 4

Business Case Solution Topology



Based upon standard product list pricing, the cost per Cisco ONS 15530 is US$205,350, resulting in an initial capital acquisition cost of US$410,700. The estimated lease cost of a 10-year dark fiber network is US$667,000. Equipment and connectivity costs for the secondary (backup) site is US$321,000, resulting in a total solution cost of approximately US$1.4 million (Table 3).

Table 3. Business Case Solution Pricing

Solution Costs Metro Network—Backup Data Center Connectivity	
Equipment	
2x Cisco ONS 15530 Platforms ($205,350 per Platform)	$410,700.00
Facilities	
Dark Fiber Network Lease, including:	$667,000.00
Initial Setup Costs	$131,000.00
Construction Costs	$200,000.00
Right-to-Use Costs for 10 Years	$336,000.00
Remote Secondary Backup Site Connectivity	
Equipment	
2x Cisco 7200/7400 Series 1 Gbps FCIP Adaptor ($10,500 per Adaptor)	$21,000.00
Facilities	
PTP T3 Circuit ($25,000 per Month)	$300,000.00
Total Cost	**$1,398,700.00**

Table 4 lists solution payback periods and associated ROIs for a range of recovered revenue that varies between 0.1 and one percent of total annual revenue. All these results are based upon the solution cost of US$1,398,700 and have an associated payback period of less than one year, regardless of the percentage of revenue impacted by unplanned downtime.

Table 4. Business Case Solution Payback Period and ROI Results

Global 1000 Annual Revenue	$3,470,000,000	Server + Network + App Impact	Related Payback Period (Days)	ROI
.1% of Revenue	$3,470,000	$2,411,650	212	72%
.2% of Revenue	$6,940,000	$4,823,300	106	245%
.3% of Revenue	$10,410,000	$7,234,950	71	417%
.4% of Revenue	$13,880,000	$9,646,600	53	590%
.5% of Revenue	$17,350,000	$12,058,250	42	762%
.6% of Revenue	$20,820,000	$14,469,900	35	935%
.7% of Revenue	$24,290,000	$16,881,550	30	1107%
.8% of Revenue	$27,760,000	$19,293,200	26	1279%
.9% of Revenue	$31,230,000	$21,704,850	24	1452%
1.0% of Revenue	$34,700,000	$24,116,500	21	1624%

These benefit calculations assume recovery of 100 percent of impacted revenue. But what if that is not the case? Additional results show that a solution payback period of less than one year still exists for all but a few of these exceptions. These are represented in the unshaded area of Table 5 and include cases in which less than 50 percent of 0.1 percent of impacted revenue (US$2,411,650), less than 30 percent of 0.2 percent of lost revenue (US$4,823,300) and less than 20 percent of 0.5 percent of impacted revenue (US$12,058,250) is impacted. For all other cases (including all those in which more than 50 percent of the impacted revenue is recovered), a less than one-year payback period still applies.

Table 5. Business Case Solution Payback Period by Percentage of Recovered Revenue

	Percentage of Recovered Revenue				
Impacted Revenue	**10%**	**20%**	**30%**	**40%**	**50%**
$2,411,650	$241,165	$482,330	$723,495	$964,660	$1,205,825
$4,823,300	$482,330	$964,660	$1,446,990	$1,929,320	$2,411,650
$7,234,950	$723,495	$1,446,990	$2,170,485	$2,893,980	$3,617,475
$9,646,600	$964,660	$1,929,320	$2,893,980	$3,858,640	$4,823,300
$12,058,250	$1,205,825	$2,411,650	$3,617,475	$4,823,300	$6,029,125
$14,469,900	$1,446,990	$2,893,980	$4,340,970	$5,787,960	$7,234,950
$16,881,550	$1,688,155	$3,376,310	$5,064,465	$6,752,620	$8,440,775
$19,293,200	$1,929,320	$3,858,640	$5,787,960	$7,717,280	$9,646,600
$21,704,850	$2,170,485	$4,340,970	$6,511,455	$8,681,940	$10,852,426
$24,116,500	$2,411,650	$4,823,300	$7,234,950	$9,646,600	$12,058,250

SUMMARY AND CONCLUSIONS

Centralized data centers help enterprises achieve substantial productivity gains and cost savings. These data centers house mission-critical applications, which must be highly available. Therefore, demand on data centers is higher than ever. Data-center design must focus on scalability and high availability. A disaster in a single data center that houses enterprise applications and data can cripple an enterprise's ability to conduct business.

Important enabling technologies such as asynchronous storage replication, disk mirroring, Fibre Channel, SANs, Gigabit Ethernet, SONET, and DWDM can support effective, economical solutions that significantly reduce unplanned downtime. Fundamental to the collective utility and value of these technologies is a shared network infrastructure where each technology can be deployed in a way that optimizes availability and maximizes performance. In contrast to the use of traditional high-speed technologies such as ATM for recovery site access, the Cisco solutions have significant cost advantages for supporting both initial and incremental business continuance. The incremental costs of adding new transport technologies to support additional recovery requirements are low because the Cisco ONS 15530 platform, its access and trunk ports, and the leased dark fiber network are already in place. This results in a significant cost advantage for the DWDM approach versus one that deploys additional ATM or other broadband circuits to support additional system or storage transport.

The network infrastructure is in place to support incremental asynchronous backup to centralized storage (either in the primary or backup data center) from multiple remote locations as needed, reducing the cost of backups and storage management. These benefits can be significant and are incremental to the advantages of reduced downtime.

Corporate Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

European Headquarters
Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: 31 0 20 357 1000
Fax: 31 0 20 357 1100

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-7660
Fax: 408 527-0883

Asia Pacific Headquarters
Cisco Systems, Inc.
168 Robinson Road
#28-01 Capital Tower
Singapore 068912
www.cisco.com
Tel: +65 6317 7777
Fax: +65 6317 7799

Cisco Systems has more than 200 offices in the following countries and regions. Addresses, phone numbers, and fax numbers are listed on **the Cisco Website at www.cisco.com/go/offices.**

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica Croatia • Cyprus • Czech Republic • Denmark • Dubai, UAE • Finland • France • Germany • Greece • Hong Kong SAR Hungary • India • Indonesia • Ireland • Israel • Italy • Japan • Korea • Luxembourg • Malaysia • Mexico The Netherlands • New Zealand • Norway • Peru • Philippines • Poland • Portugal • Puerto Rico • Romania • Russia Saudi Arabia • Scotland • Singapore • Slovakia • Slovenia • South Africa • Spain • Sweden • Switzerland • Taiwan Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela • Vietnam • Zimbabwe

KC/Pa/LW6236 07/04

Printed in the USA