Cisco Systems

White Paper

Data Center Networking Solutions

Executive Summary

It is well understood that an organization's ability to utilize information technology and the Internet to achieve productivity gains, streamline business processes, and improve customer satisfaction are fundamental to a company's short-term and long-term success and profitability. In today's current economic climate the IT organization is tasked with the ongoing central role of helping achieve these goals and at the same time finding ways to reduce IT's own capital and operating expenses. Data centers are at the core of the IT infrastructure, providing controlled environments for the centralization of critical computing resources. Typically responsible for about 50% of the IT budget[1] and growing fast to keep up with business demands, data centers have become a key area where substantial efficiencies can be achieved. Many IT organizations are undertaking numerous initiatives to evolve their data center infrastructures to achieve improvements in productivity, while at the same time improving business resilience and higher levels of flexibility and agility.

Productivity: Over the last couple of decades companies made technology investments that met their immediate needs and business objectives. The result is isolated investments in a wide diversity of applications, systems, architectures and networks that are complex and expensive to manage and administrate. IT organizations are coming to realize that they need to optimize, consolidate and standardize data center infrastructures to achieve a lower cost of ownership and focus limited capital and skilled resources on achieving their strategic goals. The IT industry has already benefited from the numerous advantages associated with a common networking protocol—IP—proving that this model can lead the way for the evolution of the data center.

Resilience: Diversity and complexity bring additional challenges associated with achieving the "always on" service levels required by businesses today. Achieving business resilience in the face of disruptions caused by natural disasters, planned or unplanned downtime, administrator errors or malicious internal or external cyber attacks is made exponentially more difficult by the additional complexity associated with infrastructure diversity. The first step IT organizations should take in achieving a resilient data center infrastructure is to evolve diverse and disparate environments into a more homogenous and structured framework. This enables a more deterministic response to disruptions; effective operational best practices and ensures less chance of human error due to increased focused expertise. The next step IT departments should take is to lead in the development of appropriate business

1. Meta Group 2003

continuance plans, procedures and solutions that effectively replicate data and systems at remote data centers to meet business needs and mitigate risk of lost data or lengthy downtime. Finally, to ensure that the data center and the hosted applications and data are secure from external and increasingly also internal breaches, security officers should define security policies that address the assessed risks. Based on these policies, the security and network operations groups can work together to secure the data center, creating secure domains derived from risk assessment results.

Agility: One of the main causes for the deployment of the diverse mix of application environments was the need for IT to respond quickly to new business requirements. By deploying isolated application environments that met the specific business needs of particular functional groups or business units, IT could respond quickly and nimbly, reducing the time to deployment. However, the unfortunate cumulative effect of deploying disparate systems is now quite the opposite. IT organizations are finding it increasingly difficult to respond quickly to business needs with such large and diverse deployed infrastructures to maintain. Moreover, isolated application islands create obstacles as companies attempt to automate cross-functional business processes within their organizations and with business partners. To enable improved agility, IT management must make efforts to standardize, optimize and consolidate infrastructures in an effort to free up valuable personnel, and provide a flexible platform for new application deployments.

Some industry analysts believe that ultimate data center productivity, resilience and agility would be best achieved through a service model that allows data center resources to be provided "on demand." For many companies that have a large installed base of diverse systems and no current plans to build a completely new data center this may seem like a vision of the future that is not currently attainable. Nevertheless, some forward thinking companies are beginning to look at how they can evolve their existing infrastructure to such a model. It is well worth considering how pending data center infrastructure investments can be made in the context of eventually achieving a services model.

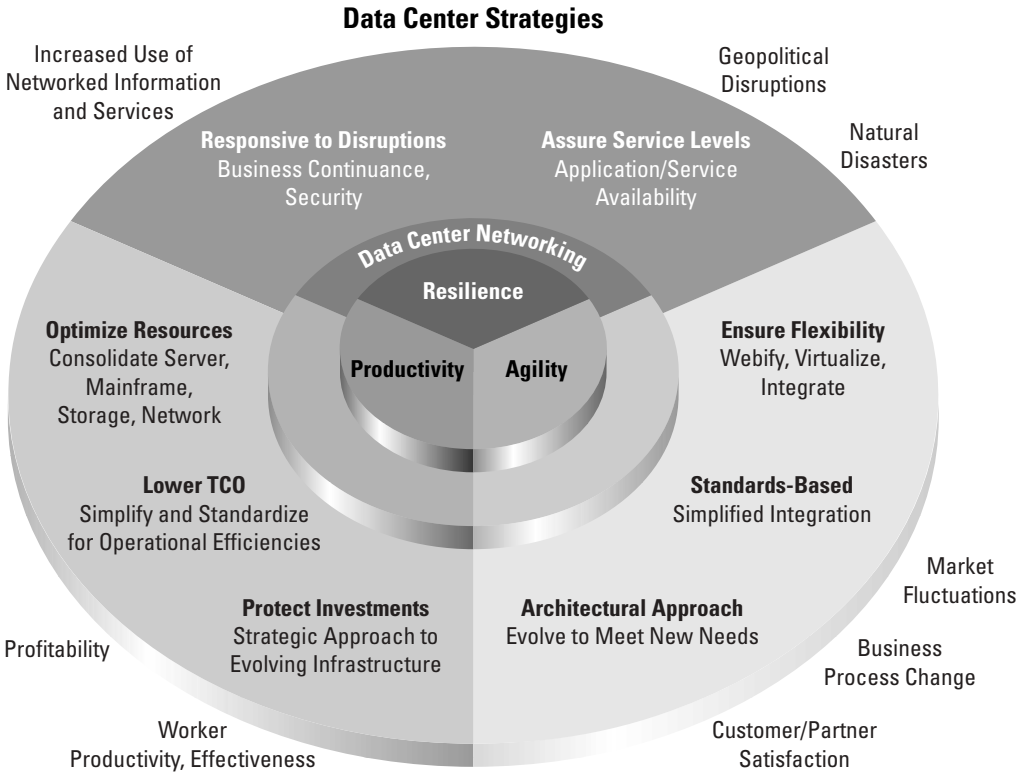
Data Center Initiatives

Most IT organizations are moving forward with a number of separate but inter-related initiatives that are tied to the data center environments to meet their goals of improved productivity, business resilience and agility. The following data center related initiatives and trends identified as top priorities by CIOs and IT executives today:[2]

- Consolidation: Servers, applications, storage and data centers are being consolidated to achieve resource optimization and lower total cost of ownership (TCO)
- Business Protection: Securing information and applications against directed or indiscriminate malicious attacks
- Business Continuance: Minimizing planned/unplanned service downtime or data loss
- Optimized Architectures: Web-based and thin-client to extend applications to broader internal and external user sets for both open system and mainframe environments
- Investment Protection: Deploying scalable, flexible infrastructure that can continue to serve changing application requirements for extended periods.
- Extending Life of Existing Investments: Evolving existing resources such as mainframes and client-server applications to Internet enabled applications

2. Various sources including Morgan Stanley 2002 CIO Survey and Yankee Group 2002 CIO Priorities

Figure 1
Business Issues Drive Data Center Strategies



Data Center Networking:

As companies embark upon one or more of these initiatives, they need to develop a networking strategy that will support the specific initiative goals as well as longer-term strategic data center goals. Data center networking describes a strategy for creating a highly available, flexible, scalable and secure networking infrastructure within data centers and between data centers that can support the goals of IT and of the organization as a whole. If executed correctly a data center networking strategy can provide the following benefits:

- Reliable user access to data center applications, services and data from wherever the user is located and whenever access is required
- Appropriately secured data center environments to protect applications and data against internal and external breaches
- Optimized application and server performance, for enhanced user experience.
- Highly available and secure interconnection of computing resources, such as servers and storage within the data center.
- Enhanced application availability and scalability through interconnection of distributed data center front-end and back-end resources over campus, metropolitan and wide area environments.

Cisco Data Center Networking:

Cisco provides IT organizations the networking solutions needed to achieve all of the above, and is committed to working with partners to help customers evolve their data center networking infrastructures to meet near-term and long-term data center goals. Cisco can help customers achieve their goals with incremental upgrades to existing networking infrastructure as well as by providing proven and validated end-to-end data center networking blueprints for completely new data centers where appropriate. Cisco data center networking solutions provide a reliable, secure and application-aware network environment that enables user access to applications and data, interconnectivity between server and storage computing resources as well as interconnectivity between data centers. These solutions are tested, validated and documented to facilitate faster and easier deployment with lower risk. The networking solutions Cisco provides for the data center help IT organizations achieve the availability, performance and security needs of mission critical applications. These solutions are open and standards-based so that all customer computing environments can be supported. In addition, Cisco is working with some of the leading infrastructure and application vendors to help enhance deployment of some of the market leading environments. This paper provides an overview of how Cisco's data center networking solutions can address all aspects of customers' networking requirements as IT organizations embark on imminent data center initiatives, while at the same time creating the strategic foundation to meet longer term goals.

Data Centers—Challenges and Trends

The Data Center

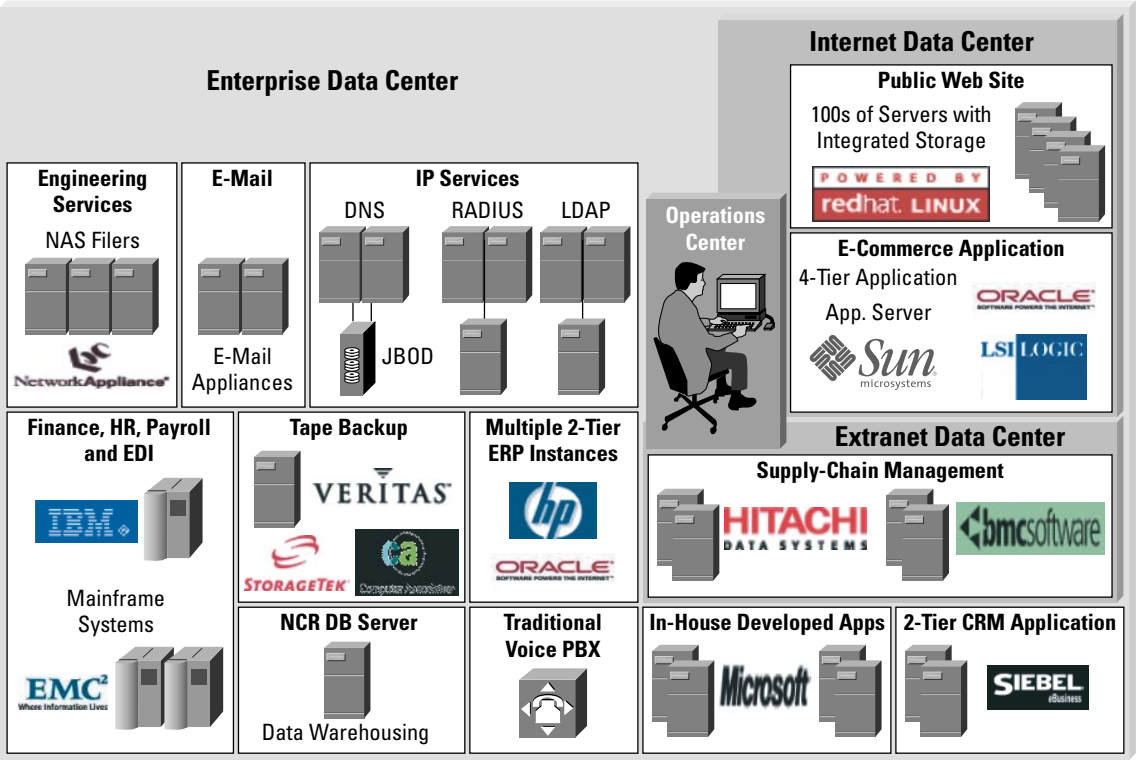
Originally the data center was associated with the closely regulated "glass house" environment of the mainframe computer, where operators would manage the jobs and provide users with the outputs. As open system environments became business critical, open system applications also migrated to the data center where they could receive the same care and attention. The data center is tasked with ensuring the availability, performance, security and integrity of applications, services and information, and housing many diverse applications for many diverse business groups. For these reasons, it is easy to comprehend why the data center is considered to be the heart of any IT operation's organization.

Data Centers are typically comprised of the following components:

- **Enterprise applications** run the business. The trend is to centralize applications such as Enterprise Resource Planning (ERP), Customer Relationship Management (CRM), Supply Chain Management (SCM), datawarehousing and e-commerce, enabling organizations to be managed as a single, virtual organization.
- **Communications applications** allow employees, partners and customers to communicate and collaborate most effectively, regardless of location, using whatever communication channel is most convenient. Such applications include legacy telephony, IP telephony, voice-mail, e-mail, instant messaging and video conferencing among many others.
- **Computing infrastructure** such as mainframes, servers and storage systems that run data applications, communications applications and services.
- **Networking infrastructure** (e.g. switches, firewalls, routers, content switches etc.) and networking services (security, caching, DNS, DHCP etc.) that ensure reliable secure user access to applications and interconnect computing and storage resources.
- **Facilities** that provide the power, cooling, cabling and physical security.

Enterprise Data Center Infrastructure Challenges:

Figure 2
Enterprise Data Centers Today



Data Centers have evolved over the last couple of decades to meet the most pressing business needs quickly and effectively. However data center management is now rethinking the strategies required to meet current business objectives and often find they face multiple challenges. Just as no two fingerprints are identical, no two data centers are identical—however today's data centers share many common traits:

- **Isolated application islands:** Applications are often deployed as islands on separate resources and without the capability to easily intercommunicate or share data with other applications.
- **Diversity of platforms and operating systems:** Data centers house a diverse array of platforms that have been deployed as server technology evolved. These include mainframes, minis and servers running multiple flavors of proprietary operating systems including UNIX, Windows, MVS, VTAM, and more recently open source LINUX operating systems.
- **Diversity of computing architectures:** Computing architectures have also evolved from monolithic mainframe computers to multi-tiered distributed computing architectures.
- **Segregated storage islands:** Typically storage systems have been deployed behind specific application and data base servers on an "as needed" basis.

- **Isolated Networking infrastructure:** Although networking infrastructures are often the easiest systems to consolidate due to a standard IP/Ethernet protocol, many organizations find their networks have grown into isolated infrastructures in support of isolated application environments
- **Overstretched Facilities:** As the need for additional computing power and storage capacity has grown, many data centers facilities are being stretched beyond their original specified environmental capacities. Also, often data centers have been set up in real estate locations where expanding them is a very expensive proposition.

The result of these data center challenges include the following obstacles, as they relate to a company's ability to achieve productivity, resilience and agility goals:

Productivity

Unacceptable TCO: The TCO associated with managing, securing and growing separate application, server and storage environments while ensuring the appropriate level of service can place a huge burden on an organization's resources For example, typically System Administrators today manage 15-25 servers. The goal is to either increase this ratio and/or decrease the number of servers substantially.

Under Utilization of Existing Resources: Because servers, storage and networking infrastructures are all dedicated to specific applications, they are often not utilized efficiently, resulting in the underutilization of CPU processing power, storage capacity and network capacity. For example, it's estimated that the average Windows server is only at 25% peak utilization, while non-networked storage is at about 40-50% utilization.

Outgrowth of Existing Data Center Premises: Due to unexpected levels of expansion in applications and storage requirements, many enterprises are outgrowing the existing space, power and environmental resources supported by their data center premises. To address the growth, companies are either building additional data centers in the same campus, metro area, or are completely migrating data centers to remote, less costly and more stable locations.

Multiple Distributed Data Centers: Alternatively some companies are faced with a multitude of distributed server farms and data centers that have grown autonomously across the campus and at remote sites. Managing and administrating all these "small" data centers is excessively expensive.

Fragmented Data Center Operations: Data center operations are managed by separate groups, each of which operate somewhat independently. These groups are often segmented into the following operational groups: applications (often specific to each business unit or functional group), data center, storage, security, business continuance and networking. The fragmentation of operations requires separate tools and management capabilities that each group has ownership for.

Business Resilience

Application and Service Availability: An IT organization's ability to ensure the availability and quality of services it provides to its users is seriously impacted by the complexity associated with managing and maintaining many diverse environments. Standardization on fewer strategic platforms and environments is a key to improving best practices and deterministic behavior of the IT infrastructure.

New Security Threats: It can no longer be assumed that by hardening the perimeter of the enterprise with firewalls that the enterprise data center is safe from attack. Because of the numerous ways to access the network and the increasing number of external personnel, such as partners and contractors that need authorized access to specific internal systems, there is a need to harden parts of the internal infrastructure as well—especially some of the most critical resources within the data center.

Ineffective and Inconsistent Business Continuance Practices: Enterprises are challenged with implementing best practices and technical solutions that address the need to protect and archive data, and ensure an appropriately rapid return to service even in the event of a severe disruption. This becomes a much more daunting task when faced with a multitude of isolated environments, the business continuance needs of which, each need to be addresses separately.

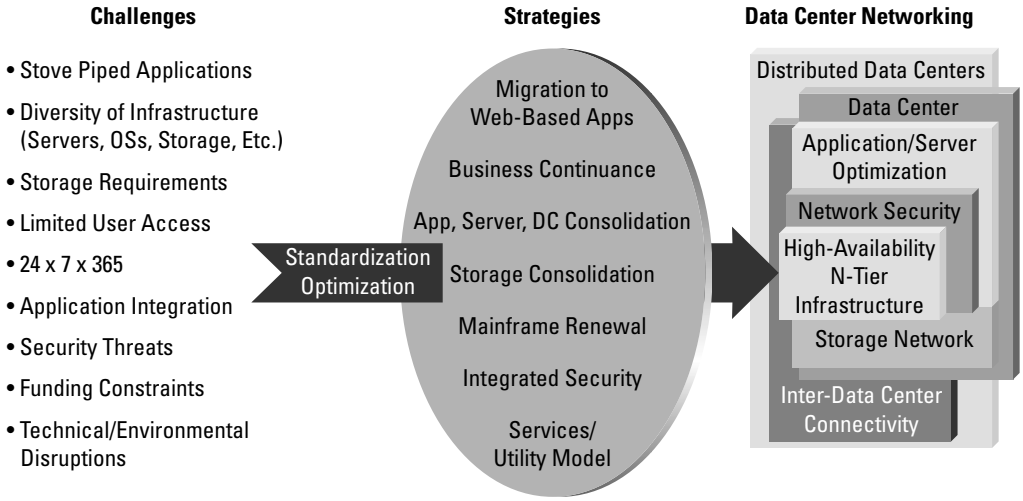
Agility

Lack of Responsiveness to Change: A fragmented and stove-piped infrastructure can be crippling to an organization's need to respond quickly to change. The investment IT needs to make to simply operate and maintain many diverse environments can preclude investment in IT projects required to enable the organization to respond nimbly and quickly to changing market conditions.

Integration of Diverse Application Environments: As businesses evolve and organizations change, there is a need to support evolving business processes across multiple applications—perhaps ERP, SCM, CRM etc. This requires much better integration between applications. This is difficult to achieve when dealing with may diverse, proprietary and isolated application environments.

Limited Application Availability: The traditional client-server environments required specialized client software on a users desktop and education of the user as to how to use that software. To better utilize and extend the software's capabilities across the enterprise, the software needs to be more easily accessible to more occasional users from diverse client devices.

Figure 3
Data Center Networking Addresses Data Center Challenges and Trends



Cisco Data Center Networking

Cisco Data Center Networking Framework

The data center network provides a foundation IT organizations can build upon to address the challenges discussed above. Customers are embarking upon numerous data center strategies in order to address these challenges. It is important to understand the strategic role networking plays in achieving these data center initiative goals successfully and expeditiously. Just as important, is to view these separate requirements in the context of a broader data center migration strategy that will enable increased productivity, business resilience and agility. The following section takes a closer look at the separate data center strategies and initiatives and the networking requirements of each. By understanding the separate initiatives, it is easier to view the data center network platform from a more holistic perspective, and ultimately architect the data center network appropriately, meeting each of the separate data center initiative requirements.

Figure 4
Cisco Data Center Networking Framework

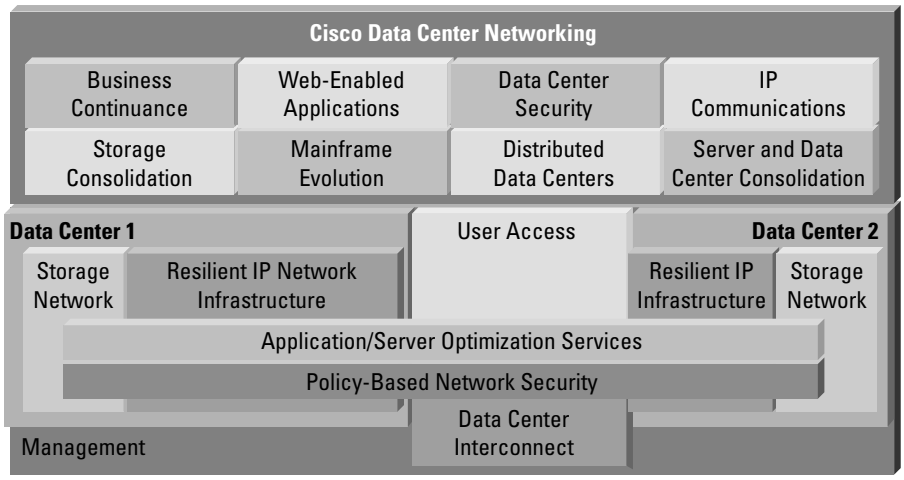


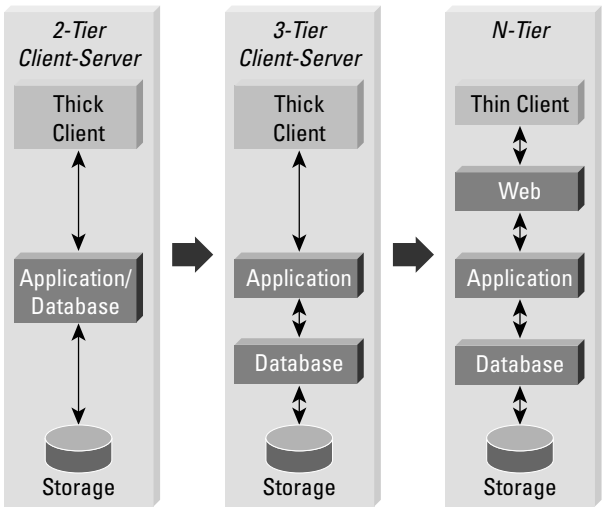
Figure 4 describes the Cisco Data Center Networking framework. The data center initiatives, such as business continuance, web-enabling applications and storage consolidation each require support from one or more of the data center networking building blocks, shown in blue. These building blocks are inter-dependant and come together to provide a complete integrated data center networking infrastructure. Some components, such as application optimization and security services span the entire infrastructure including front-end, back-end and interconnect components. A strategic view to building the appropriate networking infrastructure is to create an end-to-end data center networking blueprint that can be built out either simultaneously or incrementally to support the initiatives, as and when they become relevant to the business.

Let's begin by taking a closer look at each of the separate data center initiatives and their associated networking requirements. Then we can look as the data center network platform from a more holistic perspective, and how by building the data center network appropriately all the separate initiative requirements can be met, while also paving the way to meet future data center goals.

Web-Enabling Client-Server Applications

Many open-system applications have been deployed as 2-tier client-server applications that are relatively simple to develop, however 2-tier client server applications are difficult to scale, manage, integrate, access remotely—and require specialized client software. To address the issues 2-tier client-server applications pose, newer applications are being deployed as N-tier applications with standardized web-browser clients. In addition existing 2-tier (e.g. Oracle E-Business Suite and Siebel) deployments and 3-tier (e.g. SAP R/3) deployments are being upgraded to N-tier in order to address these issues. These N-tier applications offer greater scalability, availability and integration possibilities. Another reason driving some companies to upgrade their ERP platforms to a newer web-enabled version that supports more comprehensive functionality including SCM, CRM, PLM is the need for application integration, which these larger web-enabled packages can facilitate. Most of the large packaged software vendors are promoting these upgrades to N-Tier architectures as a way to reach a larger user population, and also as a way to integrate software functionality previously provided by smaller software vendors into their integrated platform. N-tier clients are typically web browsers or thin client implementations that either require a web browser or special generic client like Citrix or Windows Terminal Server. N-tier applications provide increased application accessibility and reach, they are easier to administer and deploy, and easier to integrate. In some cases deploying an n-tier architecture also results in a reduction in network traffic between user and data center. It also makes the applications more available to other access devices such as handhelds and PDAs. In some industries where it is preferable to only provide limited functionality to the user, the thin client allows the deployment of simple diskless stations or terminals, reducing the risk of confidentiality leaks or support issues.

Figure 5
2-Tier, 3-Tier, and N-Tier Architectures



2-Tier, 3-Tier and N-Tier Architectures

2-tier Architectures

Some of the earlier mission-critical client-server applications such as ERP used a two-tier architecture in which application processing is split into two parts between the client workstation and the server. The client runs the presentation and the majority of the application logic. The server stores the information on a database and also runs some application logic. This is often referred to as "fat client" architecture. The two-tier architecture can be more demanding on the network infrastructure because the client must download data directly from the database, resulting in high bandwidth requirements and multiple interactions between the client and server for every transaction.

Simplicity and ease of development for smaller projects is the biggest advantage of the two-tier client-server model—a model well suited for departmental applications. However because business-critical, centralized, enterprise-wide systems need to support an extended user base and broad functionality, they require the superior scalability of three-tier or n-tier architectures for both development and deployment. Hence the shift towards n-tier architectures by most enterprise software vendors today.

3-tier Architectures

In a 3-tier model, the presentation, application, and the database all reside on separate computers, delivering greater scalability, improved operations, and support for multiple client platforms.

Because most of the database inquiries are kept local to the data-center, and only presentation traffic flows across the enterprise-wide network, the 3-tier architecture offers increased performance and reduced network traffic. Scalability is also improved by distributing the application across any number of servers and enabling transaction-processing functions to funnel client requests and manage server loads.

In the 3-tier architecture, application logic is detached from the actual database, allowing for specialized application servers to be deployed using a standard interface to database servers. Since the database servers are a separate entity, they can become a shared resource among multiple applications. This model increases both manageability and portability of both the application and database tiers.

In implementing a 3-tier architecture, most software vendors developed their own presentation layer GUI software that resides on the client, and a proprietary communication protocol between the client and application software. The result was optimized communication and user interfaces, meeting the needs of a few "power users," but not scaling the application enough to be utilized by a broader set of employees, partners or customers.

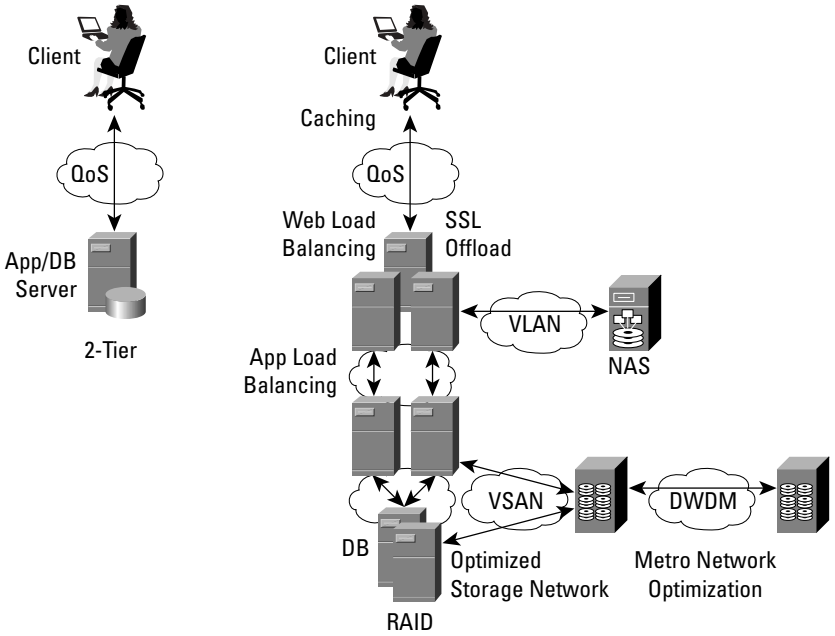
N-tier architectures

A true n-tiered web architecture separates user interface, logic, and data into four clearly delineated logical layers: physical UI rendering, logical UI definition, business logic, and data access. An n-tiered architecture provides customers with a broad variety of deployment options with UI, logic, and data being distributed amongst multiple physical tiers. This architecture offers increased performance, scalability and flexibility. There is potential to distribute and locate the physical tiers as makes sense from a performance and operations perspective. Typically, however, all physical tiers except the client are co-located in the data center. Together with the trend towards application integration and web-services, the web-enabled n-tier architecture facilitates the "virtualization" of software, such that application services are supported by a pool of application logic and database services, rather than a specific isolated application. The network is the key enabler to facilitate this evolution.

The use of a standard client web browser is a key benefit of an n-tier web-based architecture. With web architectures, organizations get the best of both worlds: they get the cost savings associated with administering a zero-install web client, and they also get the rich, interactive, productive experience available only from a desktop application.

Figure 6

Computing Architectures are Increasingly Network Centric



Data Center Networking Requirement for Web-enabled Applications:

An n-tier application is substantially more network-centric than a 2-tier architecture. In order to facilitate the deployment of an n-tier application, organizations need to design a resilient, scalable network infrastructure that secures each tier and optimizes the web, and possibly also application server tiers. The network infrastructure also needs to address the increase in storage and support the business continuance requirements.

Figure 7 describes how each component of the data center network needs to be planned to create a secure, reliable and optimized environment for web-enabled applications.

Figure 7

Data Center Networking Requirements of Web-based Applications

Application Requirements	Data Center Networking Requirements
Highly Available N-Tier Application Environment	Highly Available and Scalable Data Center Infrastructure
Scale Web, Apps and Servers	Application Optimization (Load Balancing, SSL Acceleration, Content Acceleration)
Secure Critical Data and Multi-Tier Servers	Securing the Data Center Tiers Policy-Based Integrated Security
Storage Consolidation for Improved Utilization and Backup	Storage Networking SAN and NAS Infrastructure
Business Continuance for Mission-Critical Applications	Storage Networking and Data Center Interconnect

Server and Data Center Consolidation

Server Consolidation

According to a survey commissioned by Unisys,[3] over 50% of customers are implementing or are planning to implement server consolidation. The primary goals of server consolidation are improved TCO, enhanced system management, improved service levels, higher availability and increased security.

According to Gartner Group[4] Server Consolidation can be achieved at three levels. First is logical consolidation in which the organization takes central responsibility for all servers (data center and departmental) and operating environments in the enterprise. This can often be accompanied by the physical relocation of the servers to regional or centralized data centers. Logical consolidation offers the ability to support these environments in a consistent manner, rather than have part-time business unit staff wasting their resources. It also provides the opportunity to standardize on common operating environments.

The second level is consolidation of multiple lower performance web and /or application servers running the same application, onto more powerful multi-processor servers. This is typically appropriate for NT, W2K and Linux environments, where the trend had previously been to deploy multiple low-end severs. This consolidation delivers a lower administration overhead, associated with activities such as patches, OS upgrades, security fixes, backup and storage administration.

The third level of consolidation is associated with running separate applications and services on the same server, by either partitioning the server resources or performing more advanced workload management. As more advanced features are added to achieve improved management of server resources, the result is a policy-based computing model that allows service provisioning, assurance and billing/chargeback. The eventual goal is provide these capabilities across multiple platforms—either homogeneous or even heterogeneous systems. This forms the basis for what is sometimes termed as GRID computing.

Data Center Networking Requirements for Server Consolidation:

Server consolidation is normally a major project that requires a higher performance, highly resilient network infrastructure, with enhanced security and server optimization services. In addition server consolidation also typically results in storage consolidation due to the larger storage requirement, and possibly large number of application environments running on a single server. This in turn requires deployment of a highly scalable and secure storage network.

Data Center Consolidation

In large organizations, servers were often distributed to provide local, departmental services. As these server farms grew in size and importance to the business—small-size data centers were formed. The distribution of these server farms across campuses and remote sites presents challenges for business operations and IT TCO. Having pockets of non-integrated business-critical applications and data makes it difficult to control activity and integrate business processes enterprise-wide. From an IT perspective, the resources required to manage, support and apply best practices to multiple small data centers effectively, are much greater than they would be to manage a smaller number of higher-capacity data centers. According to Gartner[5] as many as 75% of their customers are looking to consolidate

3. Unisys/Network World Server Consolidation 2002
4. Gartner Server Consolidation: A Status report—SYM 12 ITxpo 2002

smaller data centers into a few, large well-managed data centers. Companies are expecting to achieve 25% in costs (mainly in people savings) through data center consolidation. Another advantage consolidated data centers offer is they act as backup data centers for each other.

Data Center Network Requirements for Data Center Consolidation:

The aggregation of data center resources into one or more large data centers often results in major upgrades or alternatively the building of a completely new data center. The opportunity arises to evolve the existing data center network infrastructure or build a new end-to-end data center network to achieve a more easily managed, scalable, resilient and secure environment to support both front-end and back-end requirements.

Storage Consolidation

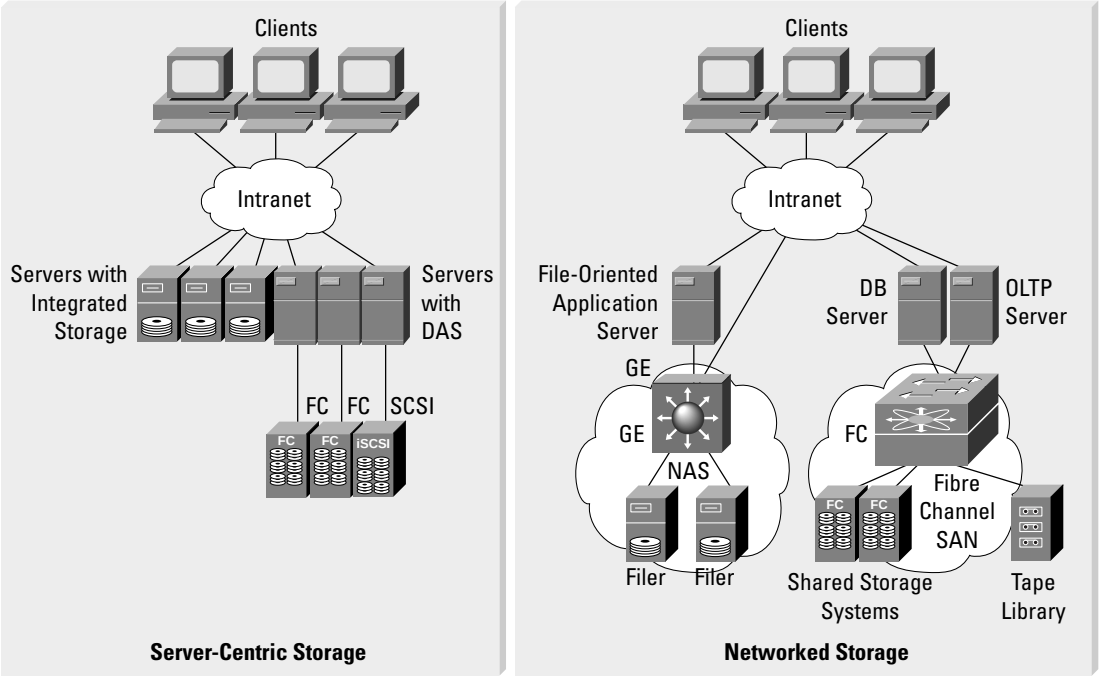
In the same way that server environments have been stove-piped, storage has been dedicated to these environments as either server-integrated storage or direct attached storage (DAS). Enterprise storage capacity requirements are rapidly expanding—on average, at rates of about 50% per year. The growth is being driven by a number of factors, including the adoption of productivity enhancing applications such as ERP, Datawarehousing, multi-channel messaging and CRM, the inclusion of rich media in new and existing applications, and an increase in demand for business continuance applications.

As customers contend with increasing storage requirements, they are compelled to find more efficient modes of deploying, administering, and protecting their storage systems. This traditional server-centric storage model (i.e. storage is internal to servers or directly attached to servers) creates many discrete environments each of which must be managed separately. The inefficiencies in storage utilization and high management costs associated with managing discrete storage environments places a high administrative burden on an organization. IDC[6] claims that by consolidating storage using network technologies and intelligent storage resource management software, administrative costs are reduced from 55% to 15% of the total cost of ownership.

Networked storage allows for storage connectivity and utilization across many servers. The resulting scalable architecture greatly reduces management complexity and Operating Expenses. The overwhelming management benefits and resulting operations cost savings are driving the rapid adoption of storage networks. The trend towards networked storage, either storage area network (SAN) or networked attached storage (NAS) is drastically improving operational efficiencies, while reducing the cost of ownership because administrators are able to manage considerably more storage capacity than was possible with the traditional server-centric model. Storage consolidation substantially improves business continuance and data protection of systems.

5. Carl Caunch Gartner 2003
6. Morgan Stanley Storage Conference 2000

Figure 8
Server-Centric Storage Migration to Networked Storage



Server-Centric Storage Results in Inefficient Management, Utilization, and Protection of Storage

Networked Storage Offers Lower Overhead, Improved Utilization, and Enhanced Business Continuance

Networked Attached Storage (NAS)

NAS provides file-level access to storage and is typically found in environments with high levels of file sharing (engineering development, motion picture production, web servers and oil and gas exploration to name a few). NAS systems (known as filers) allow access to files irrespective of the client operating system or file system (NFS or CIFS) and include features such as file-locking which in turn facilitate file sharing. Since NAS devices are integrated into the data network, they leverage Ethernet and IP for connectivity. In essence, these storage systems are attached directly to the IP network. Servers attached to the network can utilize the storage capacity of these devices. File locking insures that the data on the filer has integrity, but is still available to all of the devices on the network. For example, web server farms can store a single copy of static content in a NAS filer. All web servers have rapid access to the shared content, while updates to the content only need to be done in one place. The result is increased operational efficiencies and substantially lower management costs. This is especially important, where large numbers of low-cost servers are used to support web applications.

While some NAS vendors will argue that NAS has applicability across all applications, large transaction based applications like ERP with large databases are often better served by block-oriented SAN environments.

Storage Area Networks (SAN)

SANs provide block-level access to data and are typically found in environments where database access is integral to the business. These environments include financial trading, manufacturing, and other transaction and record intensive operations. SANs provide high availability and robust business continuance capabilities for mission critical

environments. SANs traditionally leverage Fibre Channel for connectivity, but increasingly utilize iSCSI (Internet Small Computer Systems Interface) for IP connected hosts and fiber channel over Internet Protocol (FCIP) to extend their capabilities.

Traditionally storage requirements for application and database servers were met on a per-application basis, resulting in poor storage utilization, high management overhead and availability challenges. SANs have emerged as an increasingly strategic component of the data center infrastructure that addresses the following needs:

- Scalability, availability, and maximize utilization of storage and information resources
- Streamlined administration of the storage environment
- Minimization of the TCO for storage
- Improved data availability and integrity

The rapid growth in storage management and administration costs has resulted in significant interest in moving from a direct-attached storage model to a more scalable and manageable networked storage model.

Data Center Networking Requirements for Storage Consolidation:

Storage consolidation requires the deployment of storage networking infrastructure. Depending on the application this could be either SANs for high performance transactional applications or NAS for file oriented or data sharing applications. Next generation SAN switches provide enhanced scalability, advanced intelligence, manageability and multiprotocol (Fibre Channel, iSCSI, FCIP) support.

Business Continuance

Companies embracing e-business applications need to adopt strategies that keep application services up and running 24 x 7 and ensure business-critical information is protected from corruption and loss. In the light of recent events, companies are all the more aware of the risks associated with failing to take appropriate precautions to back data up, replicate it to remote sites and have the appropriate contingency plans in place to respond quickly to any disaster. Customers need a portfolio of solutions to address the needs of different applications according to the cost associated with downtime and/or data loss.

Business Continuance is a top of mind initiative for more than 75% of enterprise customers planning to enhance their business continuance plans following September 11th.[7] According to Meta Group[8] enterprise investment in business continuance is growing at 30-40% per year and averages between 1% and 4% of IT budgets today. In order for customers to develop a business continuance strategy that ensures data can be protected and systems can be recovered rapidly, data needs to be remotely mirrored, replicated or backed up off-site. Regulations are being adopted that will make this a requirement. For example, in the financial services (Gram-Leach-Bliley Act), healthcare (HIPPA) and government (Homeland Security) segments.

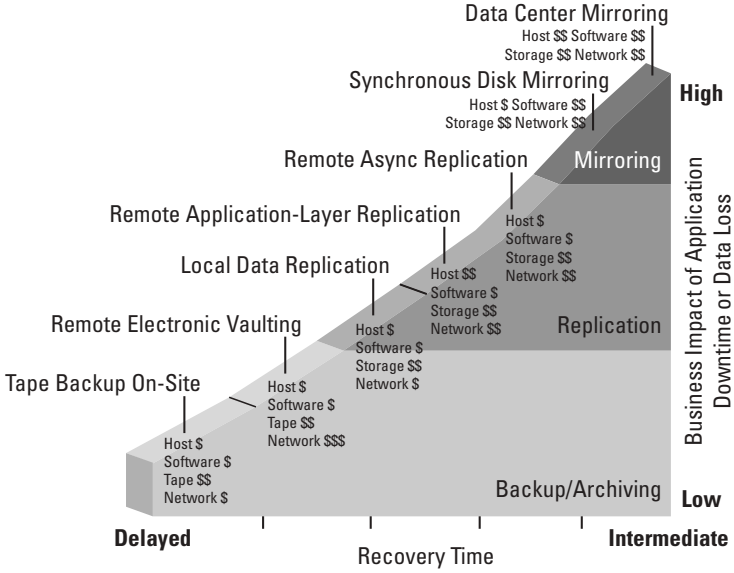
7. Disaster Recovery Journal 2001
8. Disaster Recovery and Business Continuity Planning: Key to Corporate Survival

Because downtime or data loss associated with different applications and services will impact the organization differently, customers need a portfolio of business continuance solutions to choose from. These solutions will have different associated costs and enable different Recovery Point Objectives or RPO (i.e. how much data can be lost in the case of a disruption or failure) and different Recovery Time Objectives or RTO (How long can the application be down). Business management typically defines these objectives.

Figure 10 characterizes the spectrum of business continuance solutions required to achieve these different RPO and RTO objectives. For the least business-critical applications, local backup to tape might suffice. At the other end of the spectrum, for the most mission-critical applications, where a minute of downtime, or a single lost transaction is unacceptable synchronously mirrored data centers are a requirement.

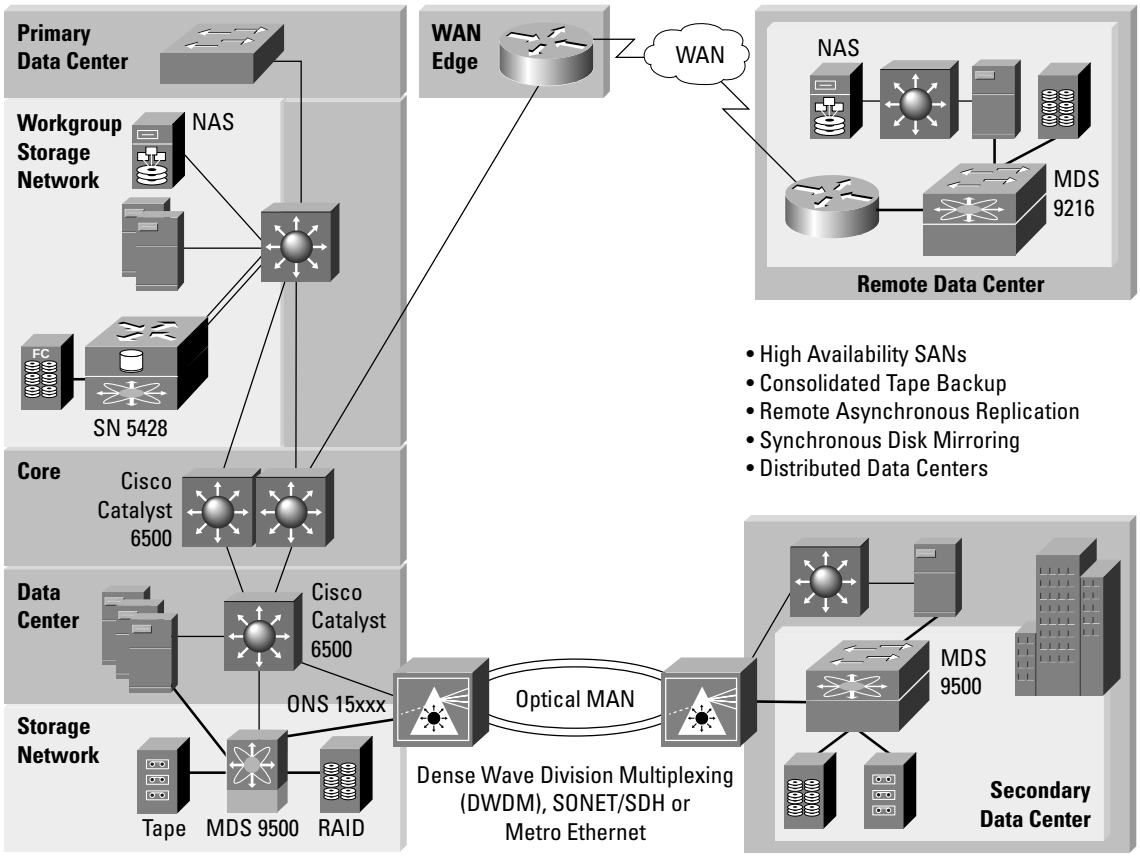
Figure 9

Spectrum of Business Continuance Solutions



Although highly desirable, it is important to realize that there is no one size fits all for business continuance. Typically companies need a portfolio of solutions, each of which fit the technical feasibility, business impact and cost criteria of different business applications. Cost and funding are key issues, however it should be observed that while the cost associated with downtime and data loss are increasing, the cost associated with achieving improved levels of business continuance are diminishing. Reasons for this include lower software and disk prices, lower costs of bandwidth and new networking technologies. Let's take a look at some of the most common strategies that should be part of a company's business continuance portfolio.

Figure 10
Portfolio of Business Continuance Solutions



1. **High availability Storage Networks:** Traditional methods of keeping data storage integrated within or captive behind a server results in a dependence upon the availability of the server for access to this data. The evolution to a networked storage environment (either SAN or NAS) ensures that failure of a server can be rapidly overcome. An alternative standby or clustered system connected to the storage network, can rapidly replace the failed system, and ensure access to the data and continued operation. In addition, a shared storage environment is more likely to support advanced RAID mirroring functionality, such that disk failures don't impact the application. By creating a scalable and reliable SAN infrastructure that can support not only the high end server systems over Fibre Channel, but also lower priced mid-range servers using traditional Ethernet networks and SCSI over IP (iSCSI), users can achieve appropriate levels of availability for all systems that provide business-critical services.
2. **Consolidated Tape Backup:** Traditionally tape backup has been the staple strategy for disaster recovery, however there are number of basic draw backs in using tape backup for systems that need to be rapidly recovered. There are questions concerning the reliability of recovery from tape, and the ability to recover rapidly not just the data, but also the systems (together with the latest patches) and applications. Also, as the amount of data stored increases, the bandwidth limitations (about 17Mbytes per second) of tape means that it is only well suited to applications where acceptable recovery times can be counted in days rather than minutes or hours. Relying purely on tape backup also results in the risk of losing all data that has changed since the previous backup. Backup is also well suited for addressing data corruption, where archived data enables clean data sets to be reloaded in the

case that data has been corrupted due to either application failures or malicious attacks. Nevertheless, backup to tape or near-line disk, in conjunction with other strategies remains an important part of any company's business continuance strategy. To ensure consistent, efficient and reliable backup and restore procedures, it is important to consolidate backup over a storage network, using backup software to schedule backups and restores to central tape libraries. The benefits of SAN-based backup, once again using either Fibre Channel or iSCSI as appropriate, include shorter backup windows and the utilization of a separate network that doesn't negatively impact normal operations. Local backups are carried out periodically to enable restores as part of the recovery process.

3. **Remote Asynchronous Replication:** For applications that require much faster recovery than can be expected from tape backup, and for organizations that require a backup site beyond typical metro environments, IT organizations should look to an asynchronous replication technique. Asynchronous replication software has been developed by storage and software vendors to use bandwidth efficiently, by only transferring changed blocks, tracks, or files– thus requiring much less bandwidth than tape backups.

   Asynchronous replication can be achieved in a number of ways. The most common method is by using software on the storage systems to replicate data changes to remote systems. This can be achieved by taking a point in time copy of the required logical units and then asynchronously copying the changed blocks to the remote site. Alternatively, some storage systems asynchronously copy or write to the remote site as the changes occur, based on the availability of bandwidth. This requires the use of techniques that can ensure the integrity of the data copy at the remote site.

   The development of new standard networking protocols such as FCIP, reduce the cost of deployment by allowing SAN extension over IP networks rather than just dedicated leased networks traditionally used for this purpose.

   An alternative to storage-based replication is host-based replication, where the server hosting the application or database logs any changes to volumes and transmits the changes to a remote host over the IP network. The remote host is then able to copy them over a SAN to the remote disk. This works well for some applications, however requires an additional remote server, is processor intensive on the production system, and needs to be implemented and managed on an application-by-application basis. Finally, more advanced NAS filer systems, typically support software that allows remote replication to be carried out in the background. Often replication can be carried out to lower performance near-line disk NAS filers, specifically intended for replication services.

4. **Synchronous Disk Replication and Mirroring:** Applications requiring the fastest recovery and—cannot afford a single lost transaction or write need to use a synchronous replication or mirroring solution. In this case all disk writes are synchronously replicated to the remote site, eliminating the risk of losing even a single transaction in the event of a production site failure. The benefits associated with this solution are fast system recovery from disk, and no-data loss. Typically, synchronous replication is achieved using advanced software on the storage systems. This software ensures that a copy of the write to disk has been successfully copied to the remote disk, before acknowledging the write operation to the application. Clearly, the drawback to this technique is the application performance impact associated with the transmission latency between the two sites. Due to the latency associated with the speed of light, the feasible distance limitation for write intensive applications, such as on-line transaction processing (OLTP) type applications such as ERP, E-Commerce, and CRM, is about 100-200km.

   An alternative to storage-based synchronous replication is host-based synchronous mirroring, where the host writes simultaneously to both the local SAN and to the remote disk, awaiting acknowledgement from both before acknowledging the transaction. Once again, distance limitations for host-based synchronous mirroring apply.

There are a number of metro technologies that are suitable for synchronous replication and mirroring. In cases where dark fiber is an option, dense wave division multiplexing (DWDM) is the most appropriate networking technology. DWDM offers the benefit of transparently transporting multiple high-speed channels (Cisco supports from 32 up to 1280 channels) across a single fiber pair. The benefit of being able to do this over distances as far as 200km, without reducing the bandwidth available to any channel (e.g. Fibre Channel receives the full 1 or 2 Gbps), allows synchronous mirroring to be achieved with a very attractive ROI. Where DWDM is not an alternative, companies can consider carrying Fibre Channel over alternative metro networks such as synchronous optical network (SONET)/synchronous digital hierarchy (SDH) or Metro Ethernet.

5. **Data Center Mirroring:** For true instantaneous failover to a backup site, IT organizations are considering creating active distributed data centers, where both the production and backup data center load share and are fully synchronized. This can be achieved in one of two ways. The first and more complex, is to load balance the same application across two mirrored sites. In this case, the users are directed by intelligent site-to-site load balancing to the most appropriate site. The second, and more common technique, is for each of the data centers to support a different set of applications, and in the case of a failure the surviving site takes over support for the applications of the failed site. In both cases this provides the highest level of business continuance (lowest RTO and RPO) by mirroring the complete data center. The cost of a completely functional second data center can be mitigated to some extent because neither data center is idle or unutilized. In addition, in an active-active scenario, there is no need to test the failover scenario, because both systems are constantly operational. Once again, latency and bandwidth requirements typically predicate a high-speed metro network that can support multiple channels for user access connectivity, system synchronization and storage replication.
6. **Technologies for Enabling Continuous User Access and Communications:** In addition to ensuring that systems are available and data is protected, there is a requirement to ensure that those systems and data are continuously and securely accessible by users who require access (employees, partners and customers). These technologies include site-to-site load balancing, virtual private networks (VPNs) and wireless LANs (WLANs). In addition telecom departments are seriously considering the benefits of distributed IP communications systems, in order to ensure continued communications, even in the case of a major disruption to one of the production data sites. Together these technologies ensure that users can access the most available data and communications services from wherever they are located. For example, if one site goes down a user can be redirected automatically to a remote site. Alternatively VPNs can be used to quickly connect a remote office to an alternate backup site, without the need for time-consuming interaction with the service provider to provision a new connection. Wireless technologies enable users to be rapidly relocated to a temporary or mobile office in the case that their primary location is no longer accessible.

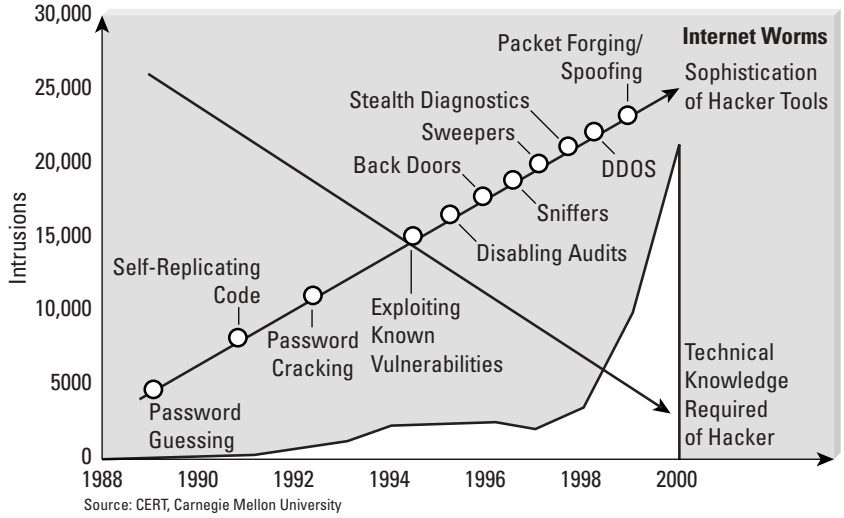
Data Center Networking Requirements for Business Continuance:

Business continuance requires a network infrastructure that is capable of reliably, securely and intelligently transporting large amount of data with strict latency and bandwidth requirements within a data center or between data centers located on a campus, within a metro area or across a wide area. The resulting network infrastructure might be intelligent SAN switches, high performance, secure IP networks, or high bandwidth, low latency metro optical networks.

Data Center Security

As we rely more than ever on IT to achieve productivity gains and competitive advantage, the potential damage that an attack on business critical systems and confidential data could cause is greater than ever. Moreover there is a worrying trend in the threats themselves. First of all, the attacks and the tools available to hackers are increasingly sophisticated. The security strategies and technologies required to deal with these threats need to be comprehensive and to provide in-depth defense. While the sophistication of the attacks is increasing, that's not necessarily true for the hackers themselves. The "open sharing" of hacking information and tools allows individuals with minimal technical knowledge to duplicate the attack. Often, it is as easy as downloading the attack tool from the Internet and launching it against targets. And finally the number of attacks is increasing exponentially. "The Computer Emergency Response Center (CERT) Coordination Center's tally topped 50,000 [attacks] by the end of 2001, more than doubling the nearly 22,000 incidents counted the previous year. Each 'incident' corresponds to a report filed by a company or organization struck by an intruder, worm, virus, or other Internet attack." These are unique attacks. "The CERT Coordination Center's policy is to count each worm or virus only once, no matter how widespread the attacks become."

Figure 11
More Attacks, More Sophisticated Attacks, Less Expert Attackers



Source: CERT, Carnegie Mellon University

Code Red and Nimda were each only counted once, although they spread rapidly and caused damage to thousands of corporations and systems. The data center itself has typically had some level of physical access security associated with it, however many IT organizations previously assumed that there was no need to protect against internal network attacks. With a growing number of methods to access the network (e.g. wireless, VPNs, WANs, dial-up,

etc.) and more people that have authorization to access specific services either remotely or on-site (e.g. consultants, temporary workers, partners, etc.), it is very prudent and necessary to consider hardening the security of appropriate parts of the internal IT infrastructure.

Data Center Networking Requirements for Data Center Security:

Security risks are present throughout the network , thus, it is critical to implement security as an integral component across the network. Some security operations managers secure the complete data center according to the policy of the most stringent application and data. Others apply a modular, zonal approach, allowing different applications and data stores to have different levels of applied security policy . In both cases, an integrated network approach that treats security as a system is needed.

To counter threats from trusted environments, an integrated, multi-layer security solution based on established policies must be deployed throughout the data center. In combination with a secure network infrastructure, high-performance security components such as firewalls, authentication servers and intrusion detection systems (IDSs) must be deployed and maintained across the data center network and also on its hosts and servers for optimal protection against threats.

Mainframe Evolution

A significant number of enterprises still count on proven mainframe technologies. Mainframe computing, long the mainstay of the centralized data center, traditionally utilizes proprietary applications based on VTAM, SNA, BISYNC, and other industry-specific protocols. Mainframe technologies and associated data networking technologies, based on IBM's proprietary SNA, provided high reliability, availability, security, and management. As data center processing and storage requirements grew, mainframes were grouped together with an implementation called Parallel Sysplex that allowed sharing of processing and storage. This architecture has evolved to Globally Dispersed Parallel Sysplex (GDPS) that now supports mainframe-based data center applications with advanced remote recovery, and scalability. Mainframes have traditionally used proprietary I/O interfaces such as bus and tag, and ESCON to access storage, and to communicate with external communications devices such as Front-end Processors (FEPs) and external storage systems. These interfaces are still prevalent in many data centers.

Although the evolution towards closer integration of the mainframe into the open systems world has been happening gradually over the last decade, more recently the mainframe has taken on a new role in the IP environment as application host and data server for e-business and Internet business solutions.

Despite the considerably higher cost of acquiring and maintaining mainframe computing versus UNIX or Intel-based computing infrastructures, many companies continue to evolve their mainframe environments in order to take advantage of the many strengths of availability, scalability and manageability that mainframes provide.

By fully integrating mainframes into the IP infrastructure and employing the intelligent network services that IP offers, organizations maximize the value of their mainframe and its contribution to business productivity, resilience and agility. This, in turn, demands high availability and reliable connections to the IP infrastructure. Mainframe connectivity has expanded to support direct high- speed LAN (Gigabit Ethernet (GE)) and storage (FICON) connections.

Data Center Networking Requirements for Mainframe Evolution:

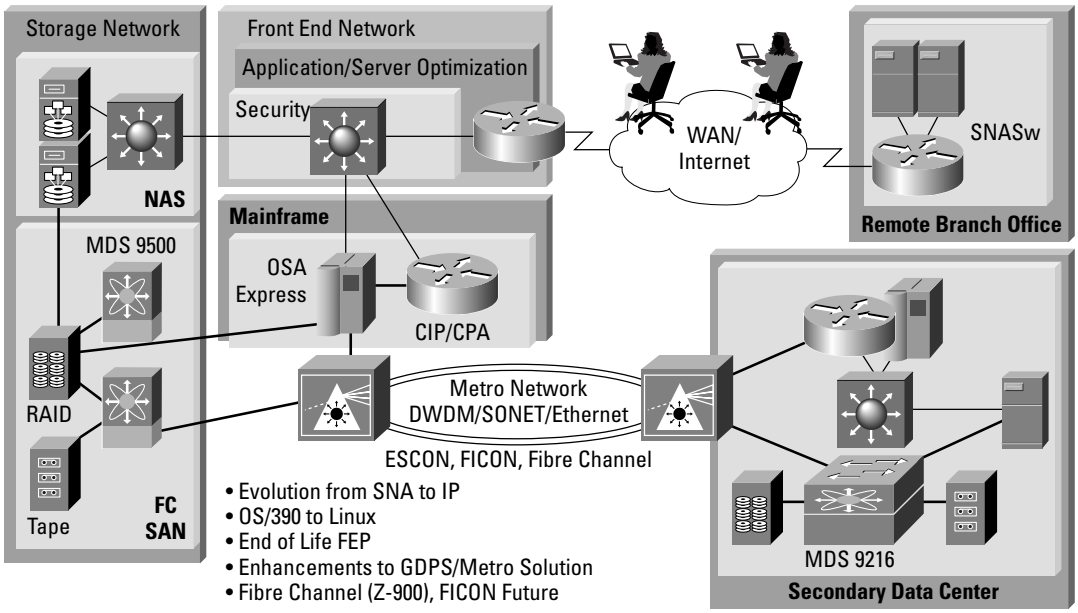
Organizations running data centers in mainframe environments need to develop migration strategies that take advantage of new mainframe IP-oriented capabilities and networking capabilities from Cisco. With the movement to support IP and GE directly on the mainframe, secure, reliable high-speed network connectivity to the mainframe is more important than ever.

Cisco supports a migration strategy with support for existing SNA and serial protocols while enabling organizations to maximize the value of their mainframes by building a robust IP infrastructure and taking advantage of its intelligent network services safely and securely. Many corporations are now in the process of replacing their IBM Communications Controller (Front End Processor or FEP) with Gigabit Ethernet switches or channel attached routers.

In addition, requirements for resilience are driving the storage and networking components of Parallel Sysplex to new levels. The addition of remote storage for data mirroring is driving optical and IP extension of enterprise system connection (ESCON) and fiber connection (FICON) disk connections. Requirements for ground data processing system (GDPS) are also driving the need to extend the necessary IBM specific protocols across metro networks.

Figure 12

Data Center Networking Requirements for Mainframe Evolution



Cisco Data Center Networking solutions for mainframe environments include:

- *Resilient IP Network Infrastructure connected to the IBM Open Systems Adapter (OSA)-Express brings the additional benefit of high-speed switching to the mainframe. Alternatively, the Cisco Channel Interface Processor and Channel Port Adapter provide direct ESCON connection to the routed network without requiring additional mainframe software, eliminating the need to manage multiple dedicated mainframe channel controllers, and offering the highest mix of WAN and LAN interfaces.*
- *SNA transport—SNA Switching (SNASw) delivers Advanced Peer-to-Peer Networking (APPN) services for SNA endpoints while eliminating APPN network node routers from the network and provides IP conversion options that support today's trend to minimize SNA traffic while maintaining native SNA functionality. Cisco Data-Link Switching Plus (DLSw+) helps customers to consolidate networks by encapsulating SNA data in IP packets and enabling SNA or NetBIOS end systems to communicate regardless of the underlying physical media.*
- *Serial protocol support—Cisco IOS Software enables integration of a variety of traditional protocols onto a single IP backbone, including Synchronous Data Link Control (SDLC), Binary Synchronous Communications (BSC), and asynchronous protocols.*
- *Support for data center interconnect over metro optical networks is optimized over a dense wave division multiplexing (DWDM) infrastructure. This enables multiple ESCON, GE and FICON channels to share the same fiber media across a high availability ring configuration.*

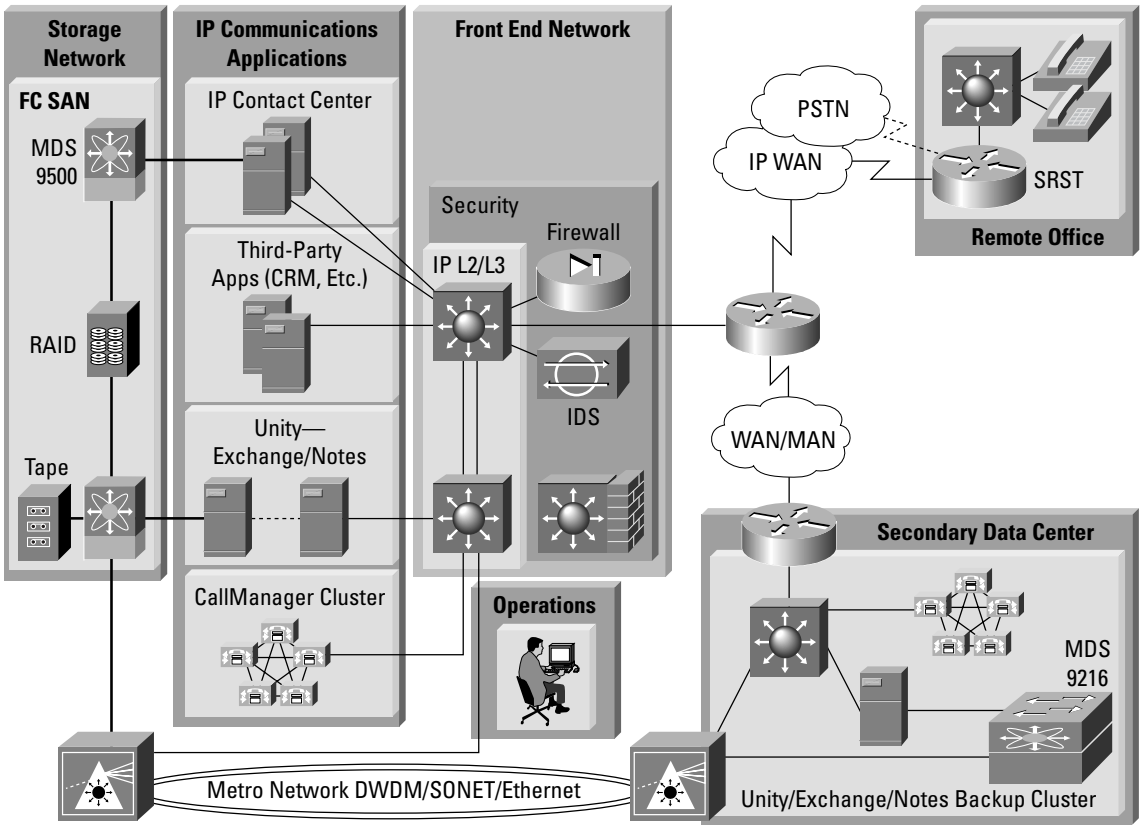
Evolution to IP Communications

The progression from proprietary systems to consolidated, open-system infrastructures that has occurred for data applications now also extends to communications. Traditionally, voice communications has been controlled by proprietary hardware (private branch exchanges [PBXs]), running proprietary software. Voice traffic has been carried on dedicated circuit switched networks (PBX networks) or networks made up of private lines and time-division multiplexers (TDMs). However, as business productivity and agility become increasingly important in today's global economy, standardization, flexibility and scalability of data and communications infrastructure are ever-more critical. As a result, businesses are looking to IP Communications systems and converged, multi-service networks to manage their voice, video, and data traffic.

IP Communications (IPC) is a comprehensive system of convergence-based solutions (including IP Telephony, IP Contact Center, Unified Messaging, and IP Audio/Video Conferencing) that dramatically improve operational efficiencies, increase organizational productivity, and enhance customer satisfaction to create an empowered, effective work environment and to deliver a measurable return on investment.

As defined by the Cisco IP Telephony Centralized Call Processing deployment model, IP Communications applications reside on multi-purpose data center servers as opposed to separate, proprietary boxes (i.e., PBXs) which were traditionally maintained by a separate staff (see Figure 14).

Figure 13
IP Communications in the Data Center



Some important things to note from this model are as follows:

- The Cisco CallManager servers are represented in the data center application pillar instead of as a separate proprietary PBX box. Placing the telephony call control software into a general purpose server allows the data center to host the voice network infrastructure using the same tools and even resources as any other data center application resulting in improved operational efficiencies.
- The MS Exchange and Notes servers are also part of the Data Center applications pillar. Centralizing the voice messaging onto the Data Center's existing email servers is another example of how Cisco IP Communications integrates with existing enterprise applications and existing operations of the data center instead of requiring a separate set of proprietary systems with separate management expertise as in a legacy TDM PBX.
- Even the contact center applications and call management control software are running on general purpose servers that integrate with existing data center network storage, and third party enterprise applications (e.g., CRM, ERP, SFA).

The IP communications infrastructure benefits from ubiquitous nature afforded by the IP network. The IP communications infrastructure can be architected to provide centralized functionality and access to all users, while distributing processing in local or remote clusters for maximum scalability and resilience.

Data Center Networking Requirements for IP Communications:

To ensure that the Data Center infrastructure effectively supports IP Communications applications, several Data Center networking provisions must be in place. These provisions, which allow enterprises to rapidly and effectively deploy and utilize these business-impacting applications, include the following:

- *Consolidated, resilient IP network—ensures the reliability of communications set up and teardown, continuous access to messaging, collaboration and contact center applications and integration with other business-critical data applications.*
- *Policy-based security—ensures a secure environment for IP communications servers and applications, with strict authorization to administration functions.*
- *Storage networks (SAN or NAS)—enables efficient storage of multi-media communications, messaging and collaboration applications. Facilitates improved protection of communications information for enhanced business continuance.*
- *Data center interconnect—enables a truly redundant, distributed architecture for maximum up-time and resilience.*
- *Integration—data center network infrastructure also needs to enable integration with legacy communication infrastructure for enhanced investment protection and extensibility.*

Because Cisco IP Communications applications are designed to run on standard data center servers and integrate with existing data center applications, much of the same networking infrastructure used by other enterprise applications can be leveraged, resulting in substantial cost savings and improved operational efficiencies. Furthermore, management of Cisco IP Communications solutions can be accomplished by existing data center operators resulting in enhanced organizational productivity. Also data center business resilience strategies once tied to storage networking and security solutions can now be extended to voice applications.

In order to facilitate a strategic approach to building a data center network that can address all of the initiatives discussed, it's necessary to understand how the optimal data center network would be built and to work towards that goal incrementally—or as a major initiative of it's own. A cross functional team is needed to represent all aspects of the data center operations including networking, applications, systems, storage, security and management. Cisco provides in-depth technical guidelines and design documents regarding the optimal overall architectures for building a data center network foundation and for each of the separate components. The designs are intended to help customers rapidly deploy, grow and evolve their data center networks to meet the needs of these separate initiatives, and future evolutions that will undoubtedly occur in years to come. These guidelines are available to customers and partners on the Cisco web-site at www.cisco.com/go/datacenter

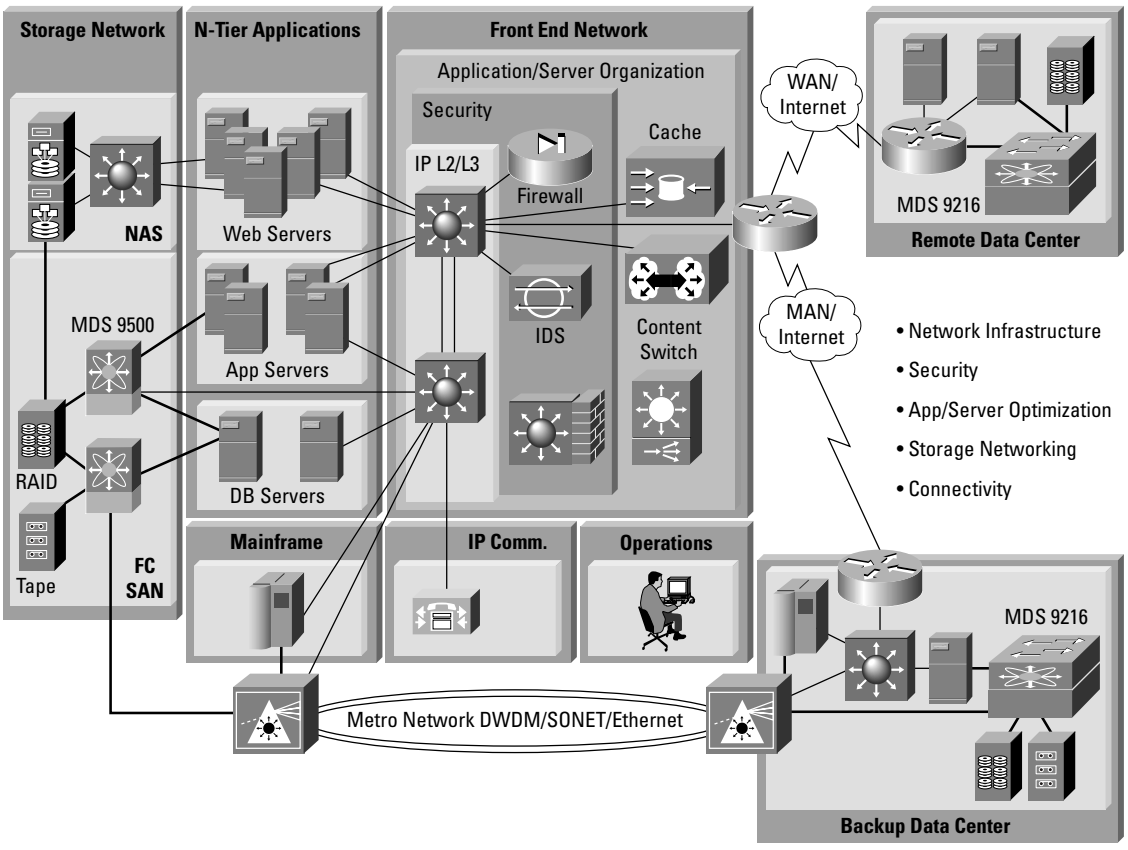
The following chapter provides a short overview of Cisco's technical solutions for Cisco Data Center Networking.

Cisco Data Center Networking Technical Solutions

Cisco has traditionally supported many aspects of the data center network infrastructure, such as mainframe SNA-IP networking, connectivity to the Internet, security, interconnectivity between servers within the data center and optical connectivity between data centers. Today, Cisco is taking a more holistic and strategic approach to meeting the networking needs of the data center and all the various data center operational groups including Security Operations, Application Managers, Storage Operations, Application Managers, the Business Continuance group and Network Operations.

Cisco Data Center Networking (CDCN) encompasses the networking foundation within the data center, as well as connectivity to and between data centers.

Figure 14
Cisco End-to-End Data Center Networking



Cisco helps IT organizations rapidly plan and build a resilient, highly adaptable data center network by providing end-to-end solutions, best practices and verified designs. The Cisco Data Center Networking Solutions Framework comprises the following components:

1. **Resilient IP Network Infrastructure** consists of highly available, scalable and intelligent layer 2 and layer 3 networking services for user to server and server-to-server communications. The layer 2 and layer 3 infrastructures are designed with integrated security and application performance in mind

2. **Integrated Policy-based Network Security** services are applied across all levels of data center infrastructure to ensure the appropriate levels of protection for applications, services and data. By taking a zonal approach to integrating appropriate levels of security into the infrastructure as dictated by the chosen security policy, Cisco data center security solutions can provide the flexibility to meet all respective application and business needs.
3. **Application and Server Optimization** services are once again applied across all levels of the infrastructure to ensure an enhanced end user application experience and optimal server utilization.
4. **Multi-layer Intelligent Storage Networking** provides servers and hosts with fast, reliable access to the storage resources they require, ensuring the best utilization of those resources. Storage networking infrastructure supports both high performance transaction oriented application and data base environments with SAN infrastructure, and file-based access and sharing, as required by file services and static web servers. Storage networking also ensures that high performance storage resources interconnect for the purposes of data mirroring and replication
5. **Data Center Inter-connectivity** provides the ability for data centers to communicate across campuses, metro or wide area distances. There are two primary goals for this connectivity. The first is to enable data centers to act as backups for each other in the case of a disruption or disaster. The second is to enable applications to inter-communicate as required.
6. **Data Center Network Management** provides a framework for data center operations personnel giving them access to the information and tools they need to work as effectively and efficiently as possible.

The following section looks at the solutions and technologies associated with each of these components in more detail.

Resilient IP Network Infrastructure

The data center IP network infrastructure design needs to be highly available, scalable and secure, as well as flexible enough to quickly address changes to existing environments or support for new environments. Other basic principals of good design include simplicity, homogeneity and predictable behavior. The IP network infrastructure needs to support a broad variety of environments including user access to applications, server-to-server communications, IP communications, mainframe communications and IP-based storage network communications. The fundamental considerations for supporting these different environments are high availability, scalability and a flexible network architecture that is designed for integrated security and application optimization services

High Availability

High availability design needs to address both unplanned and planned downtime:

Unplanned: The focus of high availability network design must be the end-user experience. The goal is to design the network and implement best practices such that any disruptions do not interrupt or interfere with end-user access to applications or services. Clearly the data center requires an extremely robust and hardened network infrastructure, however since failures do occur, any response to a failure needs to be deterministic and rapid so that it is transparent to the end-user.

Planned: While it is important to address unexpected occurrences, it is just as important to be able to address planned downtime, such as network expansions, software upgrades, memory expansions and the like. A combination of advanced availability technologies such as transparent module fail-over and best practices allow this to be done without impacting user

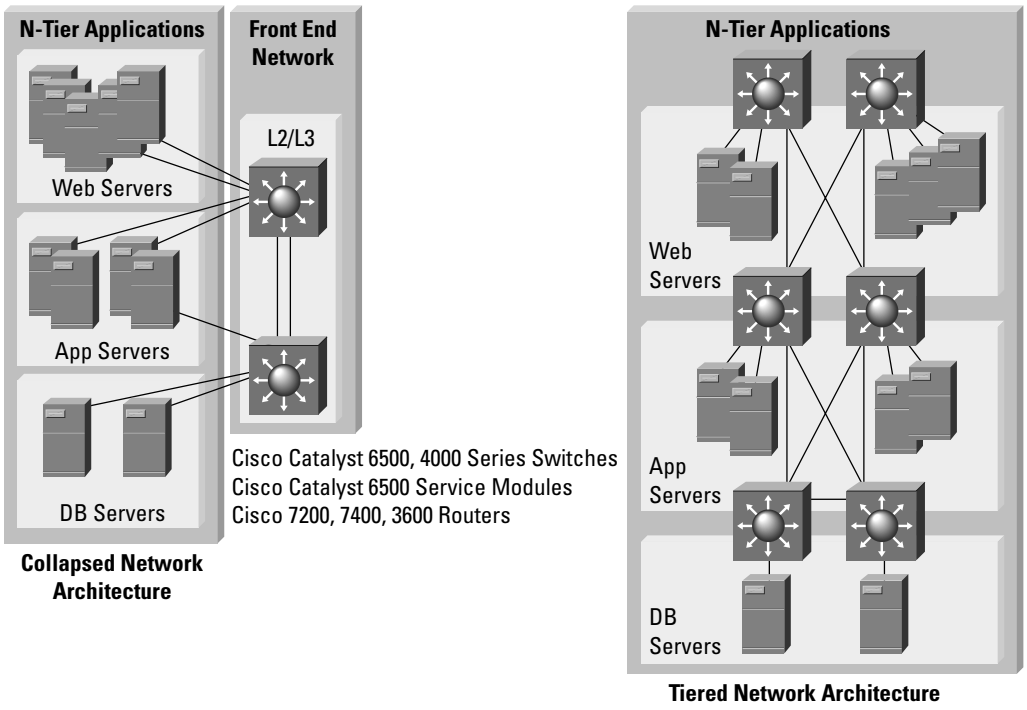
Scalability

The network must be designed to accommodate the scalability needs of the data center in terms of servers, users and bandwidth requirements, in order to meet current and future scalability requirements.- Also, the intelligent network services such as availability, security, multicast, and quality of service must scale as the numbers of users and bandwidth capacity grows.

Flexible IP Network Architecture

The network needs to be designed to meet the architectural needs of the currently deployed and future applications. Typically the network can be designed to meet the architectural needs of the most distributed n-tier architectures, such that other architectures are supported by default.

Figure 15
Resilient IP Networking Foundation



The network also needs to be designed to meet the security strategy of the organization. The organization may opt for a single security policy to meet the needs of all data center resources. Typically, IT organizations are opting for a zonal approach that provides the flexibility to associate different applications and data with different levels of security policy, that can then be applied to the security infrastructure. The network needs to be designed to support a strategy that can provide the required separation between different security zones.

In addition the network needs to support higher layer application and server optimization services such as content switching, Secure Sockets Layer (SSL) offload and caching.

Network managers need to decide whether to implement separate switches at each tier of the application architecture or whether to implement a collapsed architecture that supports all tiers on the same switches. Both cases afford the same set of logical support. An important consideration network managers need to take into account when deploying new data center services is whether to deploy service modules such as firewalls, IDS and Content Switching service modules into the L2/L3 switch or whether to use an appliance model, where such services are provided by external appliances connected to the switch. There are pros and cons for the integrated service model versus the appliance model. The general trend is towards an integrated services model, the more flexible model, because services can be seamlessly applied virtually to different segments of the infrastructure as required.

To summarize, a successful design for the resilient network infrastructure requires an understanding of a number of factors, typically outside the area of control of the network manager. These factors include the application architectures, the current and future capacity needs, and security and application optimization requirements. Because of the numerous system interdependencies, the data center network design needs to be made among all data center operational owners.

Integrated Policy-Based Security

As the central repository for business critical data and applications, the enterprise data center is a prime target for security breaches; therefore, it needs to be the first place companies look to when applying a security policy and associated security infrastructure. Traditionally security operations managers have applied a single security policy to the entire data center infrastructure, however the growing trend is to deploy a domain approach to security, where applications and data are assigned certain security policies based upon a risk assessment that considers their value to the company, confidentiality and importance. These different policy levels can then be applied to the different domains associated with those applications.

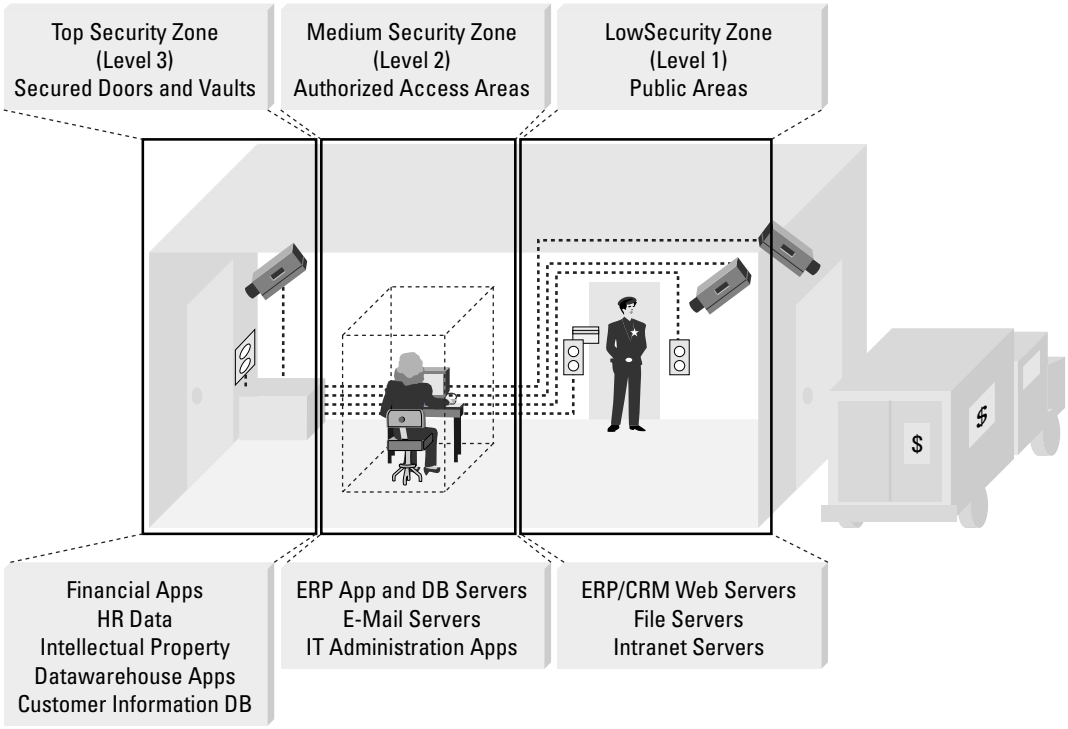
Cisco integrated network security solutions enable organizations to efficiently protect their data center networks from threats while reducing the operational costs of securing their business. Cisco provides modular, scalable, feature-rich security solutions on flexible deployment platforms. The security solutions include specialized, high-speed appliances, enhanced line card modules for routers and switches and robust software solutions integrated into the network infrastructure via the Cisco IOS® Software or offered in dedicated applications. This comprehensive product portfolio enables customers to safely deploy mission-critical business applications and services within and between their data center networks.

Policy Levels

The policy level assigned to each security zone will determine the level of safeguard is deployed within that particular zone. For example, the security zone of a mission-critical database may have the highest policy level (e.g. level 3 on a scale of 1 to 3) assigned so that it is completely firewalled except from other application servers and administrators.

When defining these network security zones, the approach should be that any security zone that is connected to a third party, such as a business partner or the Internet should always be considered high risk regardless of the data or the applications that reside within that zone. As each zone of the network is identified, you will also need to identify the associated security policy that best applies to the applications and the data within that specific zone. Each policy will touch on things such as comprised risk, potential damage to your company's image or revenue, and impact to business continuity. Many security professionals would like to see every installation secured at level 3. However, we realize that in today's world, this is highly unrealistic based on economic reality, breadth of access required, and the type of application and data that resides within the network.

Figure 16
Taking a Security Zone Approach to Enterprise Data Center Security



Integrated Systems Approach

Cisco's security solutions for the data center are integrated and end to end from the user to the data center edge all the way through to the storage network and data center interconnect. A point product approach that does neither integrates closely with other security devices nor with a securely designed network will exhibit limited effectiveness in combating the ever-increasing levels and sophistication of attacks. A legacy security solution based on a firewall that provides perimeter security is a good start but insufficient to combat the increased sophistication of external attacks, and increased likelihood of security breaches from within the network. Data center operations need to deploy an integrated system-wide approach such as that offered by Cisco.

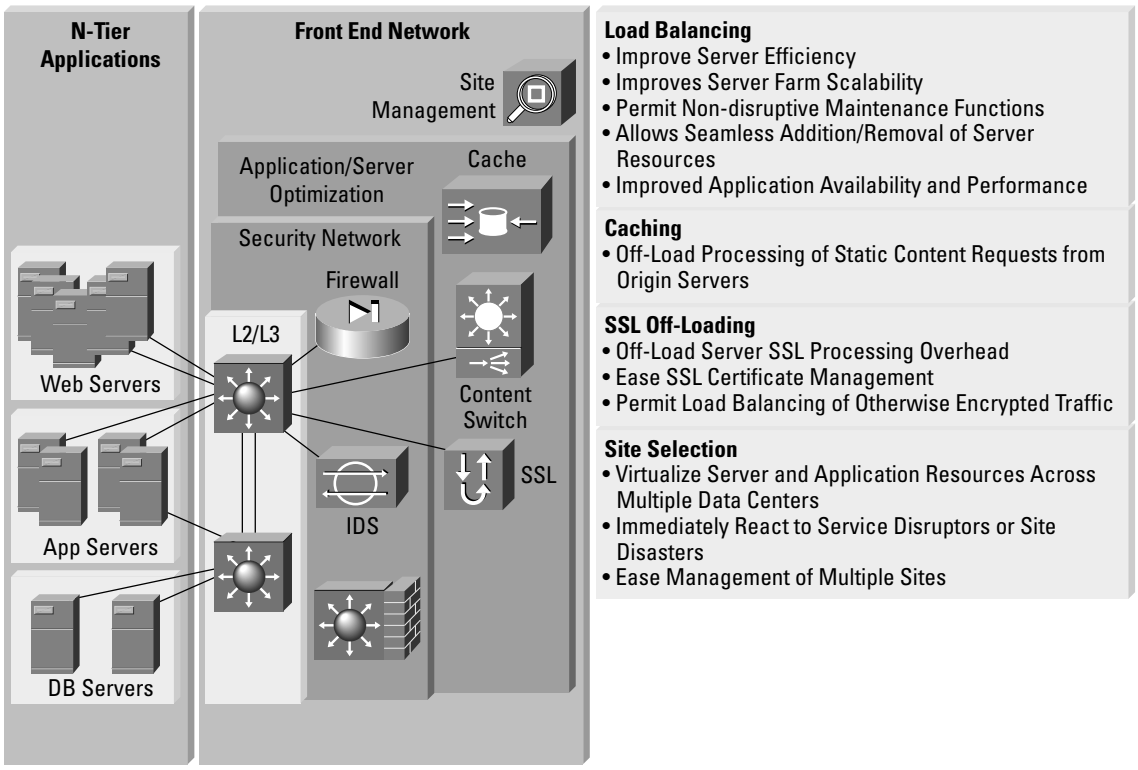
These designs leverage a broad range of technologies and solutions to provide a multi-layer security solution that can be applied to meet the policy requirements of each domain within the data center. These technologies include: Firewalls, Intrusion Detection Systems (IDSs), Virtual Private Networking VPN/IPSec, Virtual LANs/SANs (VLANs and VSANs) and Authentication, Authorization, and Accounting (AAA). These technologies should be applied depending on the type of application (Intranet, Internet or Extranet), the associated policy (high, medium and low) and the required openness and free flow of data.

Application and Server Optimization

As Web-based applications are extended to more employees, customers and partners, data center resources (e.g., servers, caches, and firewalls) must scale to meet the increasing transaction load, and must readily adapt to new demands for enhanced functionality. By deploying server and application optimization services within the data center—or across multiple data centers—online systems and resources provide for best-case availability, security, and scalability.

These services ensure that users are directed to the data center resources that can best fulfill their online service request—whether that request involves a simple download or a complex SSL-based secure transaction. Applied to Internet, intranet, and extranet e-business applications, these advanced networking services allow enterprises and service providers to provide the best possible end-user online experience; optimize the use of available resources such as servers, applications, firewalls, caching systems, and staff; and ensure the integrity of sites, systems, and transactions. Figure 18 outlines key server and application optimization services that enable the deployment of secure, scalable, resilient e-business applications

Figure 17
Application Optimization Ensures Service Quality



Given the broad range of Server and Application Optimization services offered by the Cisco Data Center Networking solution, specific areas of ROI and business benefits can vary from one organization and configuration to the next. However, the common benefits for all data centers are:

- Better website and application performance
- Best use of data center resources—servers, caches, firewalls, VPN connections
- Increased site, system, and transaction integrity
- Reduced support requirements through automation and centralization
- Enhanced online service to end users

All of these benefits translate to cost savings and improved profitability and revenue flow both in the short run and the long run.

A Focus on Key Server and Application Optimization Services

Within the data center, the most common server and application optimization services enabled by the Cisco Data Center Networking solution are:

- Load Balancing—Content Switching for Servers, Applications, Firewalls, and VPNs
- SSL Termination and Acceleration
- Content Acceleration—Data Center Caching
- Dynamic Site Selection—Multi-site Load Balancing and Site/Service Recovery
- Site & Services Management

Load Balancing—Content Switching

Content switching is a key component of the Cisco Data Center Networking solution—delivering critical optimization services such as advanced web and application server load balancing; firewall and VPN load balancing and cache redirection. Content switching works to ensure that all available resources are utilized effectively in response to a user's request for content downloads or transaction execution, providing users the best possible response times for any given transaction. From an application perspective, it is important to note that content switching services work to optimize traffic flow to and from many different applications and systems—from many different vendors.

SSL Termination and Acceleration

SSL termination and acceleration services apply to a wide variety of e-business environments and data center configurations—from the small e-commerce site to the global financial institution. Secured HTTPS exchanges (HTTP exchanges utilizing SSL encryption) are being applied to extranet and even intranet applications across many industries.

Cisco's Data Center Networking solutions provide for SSL termination and acceleration services via switch-integrated SSL services modules and standalone SSL appliances. While offering flexibility in design both types of systems provide the same SSL-related benefits:

- Off-load demanding SSL processing from servers—saving server resources
- Eliminate the need for SSL cards within servers—reducing deployment costs
- Boost SSL transaction rates and volumes—improving response times and capacities
- Centralize SSL certificate management—easing management of a secured system
- Enable continued load balancing—ensuring efficient and effective application execution

The Cisco Data Center Networking solution combines both the SSL termination and acceleration service with the load balancing service to secure user transactions and improve application and server performance, as well as to ensure that transactions execute properly and resources are fully utilized.

Content Acceleration—Data Center Caching

Content Acceleration calls for the use of caching systems as substitutes for origin servers for static content downloads. The benefits of content acceleration can be dramatic when data center applications utilize static content for screen-building or user downloads. Origin servers no longer need to respond to static object requests, lessening I/O demands on the server and freeing up server CPU cycles. This distribution of static content activity increases the performance and scalability of websites and applications—no matter if these sites and applications are available over the Internet, an intranet, or an extranet. For the end user, the result is better response times—no matter the type of content requested. For the data center manager, service levels (download times and application response times) are improved and acquisition and operating costs are lowered by leveraging caching systems in place of more expensive and complex servers.

Dynamic Site Selection—Multi-site Load Balancing and Site/Service Recovery

For larger enterprises and service providers, operating across multiple data centers provides for protection from single-site failures. In addition, potential network cost savings and service improvements can be gained by offering services closer to the end user. This distributed approach, while offering numerous potential advantages, does introduce greater complexity and the potential for resource underutilization. Success here is measured by balanced and efficient utilization of resources—systems and staff—across all data center locations.

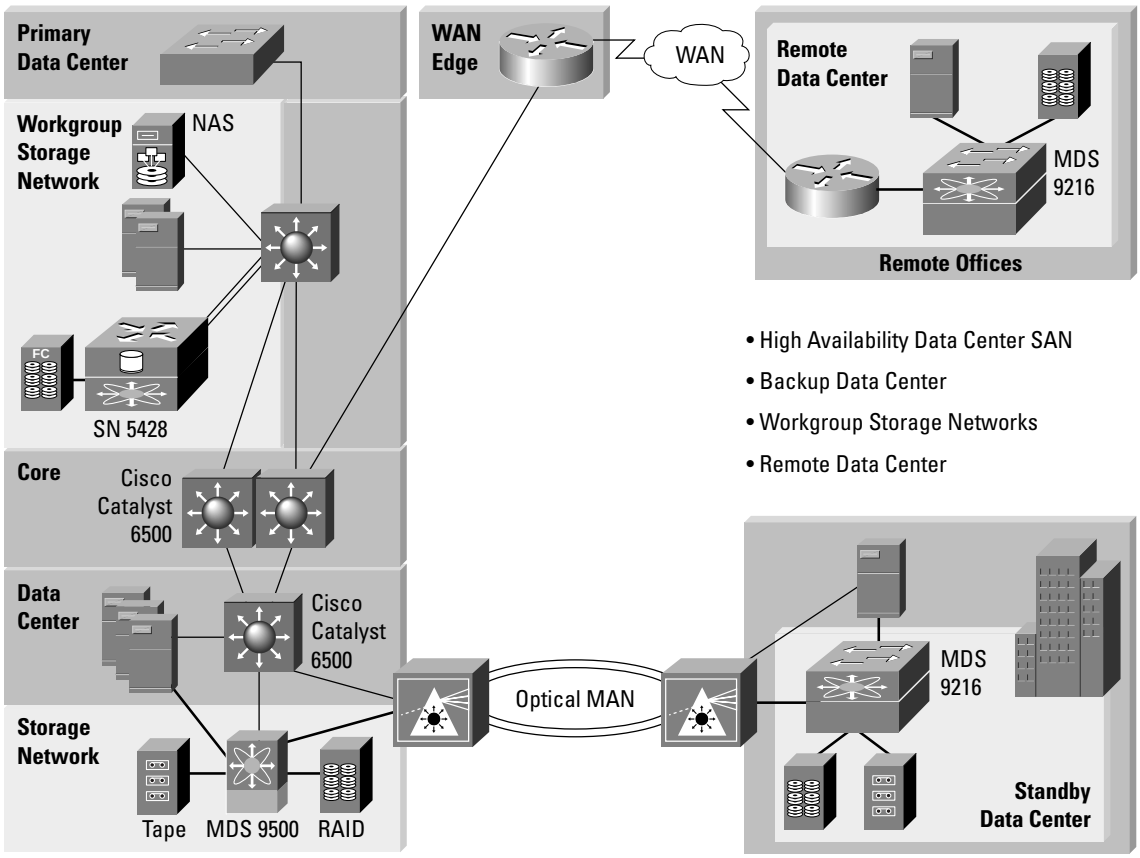
Dynamic site selection within the Cisco Data Center Networking solution provides for two critical functions: advanced multi-site load balancing and automated site/service recovery. Dynamic site selection allows organizations to deploy global Internet or distributed intranet applications with the confidence that end-user requests will be routed to the most appropriate site—according to site availability, end-user location, site load factors, and other administrator-defined traffic control parameters.

Storage Networking

Cisco storage networking solutions enable companies to realize the vision of globally networked storage by creating high performance, scalable storage networks within data centers and by also extending their storage networks beyond isolated islands in the data center to campus, metropolitan, and wide-area environments. Cisco helps organizations deploy the storage networking infrastructure most appropriate to the application and environment, whether the need is for block-based SANs or file-based NAS.

Cisco Storage Networking is a comprehensive set of technologies, products, and partnerships that provide a networked storage infrastructure based on an open architecture and industry standards. Cisco Storage Networking allows customers to adopt a strategy for accessing, managing, and protecting their growing information resources across a consolidated IP, Gigabit Ethernet, Fibre Channel, and optical network infrastructure.

Figure 18



Multilayer Intelligent Storage Solutions

Multilayer and multi-protocol intelligence are key attributes of Cisco's storage networking. From the MDS 9000 Family which supports FCP, FCIP and iSCSI and has the capability to host advanced storage applications in data centers to the SN5400 Series, which supports Fibre Channel Protocol (FCP) and iSCSI protocols for cost-effective deployment of workgroup SANs. Cisco solutions bring leading innovation and functionality to storage professionals.

- Multi-protocol Support—Multi-protocol support allows storage architects to architect a network that has the optimal balance of performance, cost and reach.
- Multi-layer Intelligence—Multilayer intelligence is achieved through intelligent network services, advanced storage services, and integrated storage and network management

Cisco is working closely with storage industry leaders to deliver best-of-breed solutions and support that enable storage consolidation and business continuance. Cisco, with the storage networking industry, is driving industry standards, technology development, and industry-wide interoperability. This effort includes standardization of new IP storage networking protocols including Small Computer Systems Interface (SCSI) over IP (iSCSI) and Fibre Channel over IP (FCIP).

Data Center Interconnect

The growing need for business continuance, application integration, storage consolidation, and data center outsourcing, requires data center operations managers to look for ways to efficiently interconnect data centers. Depending on the location of the data centers and the applications being deployed, the interconnecting network must exhibit certain, availability, bandwidth, security, and latency characteristics. The data center interconnect may be required by one or more of the system tiers, often requiring multiple connections requiring support for a range of protocols and interfaces. For example the interconnect could be used simultaneously for data replication (ESCON, Fibre Channel, FICON, FCIP), database electronic journaling (IP) and web server geographical load balancing (IP/HTTP).

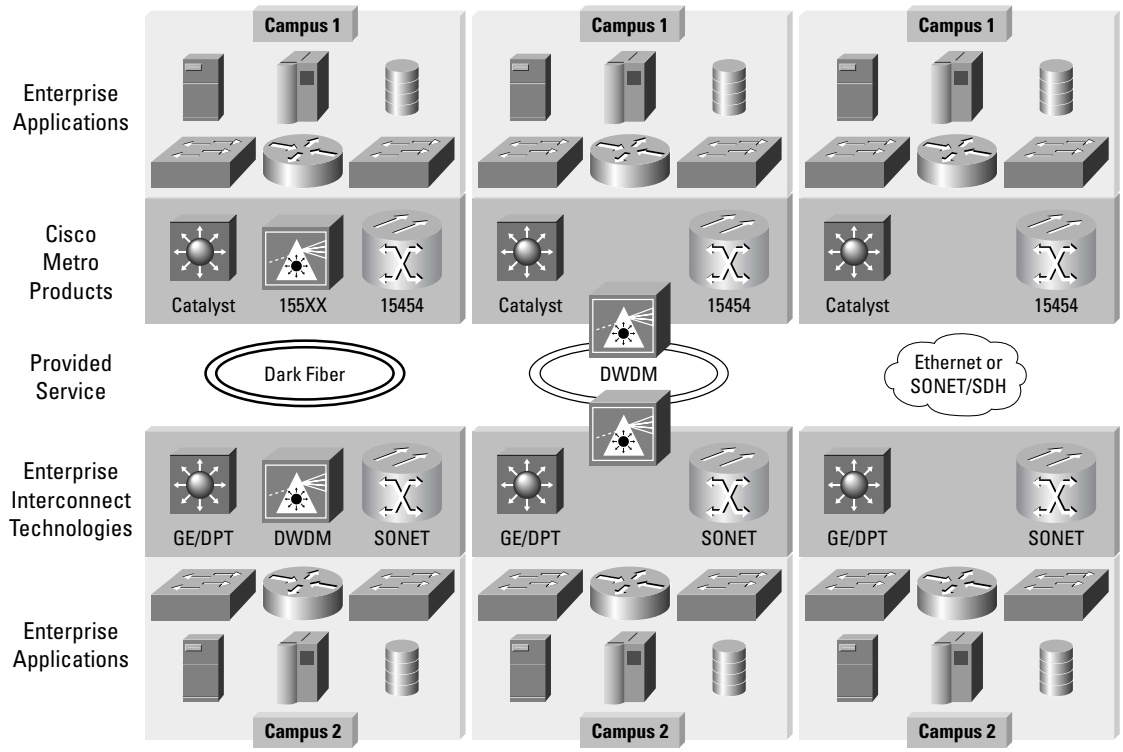
Some of these applications such as the synchronous replication, stretched clustering and mainframe synchronization exhibit latency sensitivity, and in most cases would be limited to a metro environment, while other non-synchronous applications can be deployed within the metro environment or extended over much longer distances where the limiting factor is cost of bandwidth.

Customers with data centers located across the metro area (up to 200km apart) have a number of choices:

1. If dark fiber is owned or leased companies, can set up their own metro network based on a number of technologies including:
   - Dense wave division multiplexing (DWDM)
   - SONET or SDH
   - Metro Ethernet or IP/RPR

   The choice of technology will depend on a number of criteria, including the aggregate amount of bandwidth required, protocol mix needed to be transferred and required latency and availability. Cisco provides market-leading solutions for customers to build their own metro network, regardless of which technology the IT organization decides is the most appropriate.
2. If a managed DWDM services or leased wavelength is a preferred option due to reduced administration burden, customers can build their own data center interconnect based on this transport service. For example, a SONET/SDH network can overlay a DWDM managed service to help aggregate and optimize utilization of each wavelength leased.
3. Finally, customers can choose to lease a service based on either SONET/SDH, or Metro Ethernet services. Due to generally lower bandwidths and in the case of Metro Ethernet less deterministic latencies, the types of applications that can be deployed across these infrastructures are more limited. However the distance associated with these services are generally much less constrained than dark fiber or managed wavelength services and use of new protocols such as Fibre Channel over SONET/SDH or Fibre Channel over IP (FCIP), will enable customers to address opportunities both within the metro network and beyond.

Figure 19
Choosing the Appropriate Metro Technology

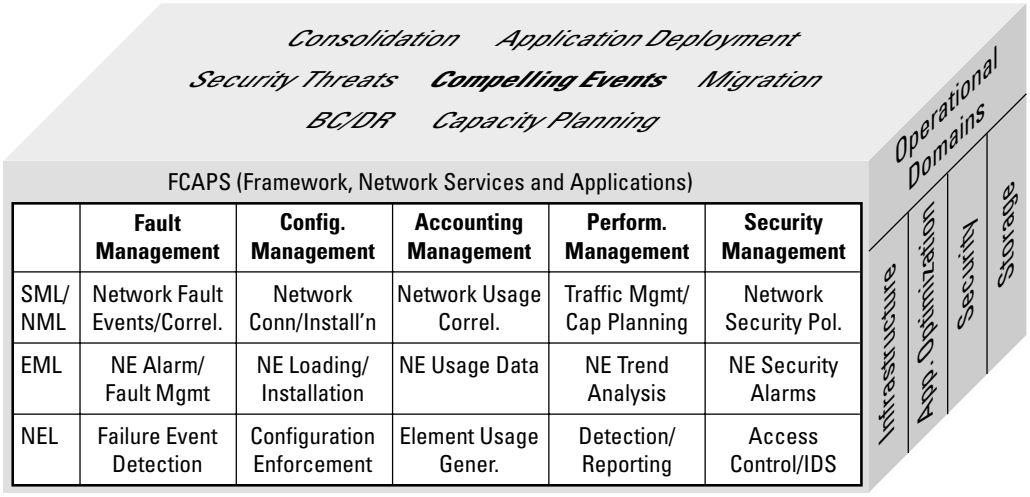


Data Center Management

To succeed in reducing operational costs while meeting service-level expectations, all the operational managers of the data center need tools that empower them to efficiently manage their environments.

Cisco's extensive network management portfolio, together with its ecosystem of partners, provides an extensive toolkit that data center professionals can use to ensure efficient fault monitoring and identification, configuration, accounting, performance monitoring, and security management. Cisco's solutions meet the needs of the multiple operational constituents in the data center, including network operations, security operations, system/applications operations, and storage operations.

Figure 20
Data Center Management Framework



	Fault Management	Config. Management	Accounting Management	Perform. Management	Security Management
SML/ NML	Network Fault Events/Correl.	Network Conn/Install'n	Network Usage Correl.	Traffic Mgmt/ Cap Planning	Network Security Pol.
EML	NE Alarm/ Fault Mgmt	NE Loading/ Installation	NE Usage Data	NE Trend Analysis	NE Security Alarms
NEL	Failure Event Detection	Configuration Enforcement	Element Usage Gener.	Detection/ Reporting	Access Control/IDS

The CiscoWorks product line provides powerful management applications to manage your end-to-end Cisco Data Center Networking infrastructure. These CiscoWorks applications improve the accuracy, efficiency, and effectiveness of your network administrators and operations staff while increasing the overall availability of your network through proactive planning, deployment, operations, and troubleshooting capability.

More specifically to address security management, Cisco's extensive security management is provided via the CiscoWorks VPN Security Management Solution (VMS), an integral part of Cisco's solutions for network security, which combines Web-based tools for configuring, monitoring, and troubleshooting enterprise VPNs, firewalls, and network- and host-based IDSs. CiscoWorks VMS delivers the industry's first robust and scalable foundation and feature set that addresses the needs of small and large-scale VPN and security

For application optimization and Layer 4-7 services, the CiscoWorks HSE 1105 Hosting Solutions Engine is a turnkey network management appliance that provides Layer 2-7 monitoring of the data-center network infrastructure and configures and activates content networking services within a Cisco-powered e-business site. HSE provides up-to-date information for operational staff to readily adjust systems to changing conditions as well as rapidly pinpoint the source of problems. In addition, CiscoWorks HSE provides custom views and secured feature access that allows multiple support groups—for example, network engineering, Web-site administration, application development, and business operations—to more effectively perform operational duties and enhance the performance and reliability of site-resident e-business applications.

Cisco also provides extensive storage networking management capabilities to deliver on the promise of more efficient storage operations. To meet the needs of all users, the Cisco MDS 9000 SAN switches provides three principal modes of management, including Command Line Interface (CLI), Cisco Fabric Manager and integration with third-party storage management tools. Cisco Fabric Manager is a responsive, easy-to-use Java application that simplifies management across multiple switches and fabrics. Cisco Fabric Manager enables administrators to perform vital tasks such as topology discovery, fabric configuration and verification, provisioning, monitoring, and fault

resolution. All functions are available through a secure interface, enabling remote management from any location. Cisco Fabric Manager may be used independently or in conjunction with third-party management applications. Cisco provides an extensive API for integration with third-party and user developed management tools.

Partner Solutions

Cisco AVVID Partner Program

The Cisco Architecture for Voice, Video and Integrated Data (AVVID) Partner Program extends the value of Cisco Data Center Networking by augmenting it with 3rd party technologies and products, enabling complete solutions to meet evolving business needs.

By achieving this interoperability through a broad range of integration interfaces, including application programming interfaces (APIs), protocols, and industry standards, the Cisco AVVID Partner Program ensures that a broad choice of multivendor solutions are available to complement the core data center networking infrastructure offered by Cisco.

Cisco AVVID Partner solutions, developed and tested for interoperability with Cisco network technology, enable customers to:

- Improve business productivity through accelerated deployment of business applications and solutions
- Bring resilience to mission critical applications by implementing standards-based, open architectures
- Benefit from an agile network infrastructure enabling them to meet changing business conditions

ECOstructure

ECOstructure or the EMC, Cisco, and Oracle infrastructure initiative is a collaborative effort, combining the core strengths of the three companies to provide an end-to-end data center infrastructure—technology, customer proven expertise and services. Since its inception it has delivered four major blueprints. The blueprints, which are openly available, can be downloaded from the ECOstructure web site (www.eecostructure.com), and serve as best practices documents to advise IT professionals on the integration of Cisco, EMC, and Oracle products and technologies. Customers can utilize the blueprints to do their own implementations or they can work through system integrators or consultants that specialize in ECOstructure implementations.

ECOstructure provides productivity through tested and proven architectures from three market-leading companies. The blueprints help IT designers and architects create architectures providing them with agility to respond to a changing business environment. The architectures eliminate any single point of failure across the infrastructure-to-application stack, allowing mission critical applications to respond quickly to disruptions or failures. The Remote Services blueprint is a model for providing computing as a utility; ECOstructure delivers the vision of application services coupled with remote support capabilities.

Any company consolidating its systems or streamlining its business processes with the intention of improving business productivity, resilience and agility can benefit from ECOstructure. By speeding the planning and deployment of these integrated solutions, ECOstructure helps drive cost efficiencies and eliminate risk for customers.

HP Utility Data Center

Services Model for Data Center Computing

As the data center undergoes a trend of consolidation and optimization, some industry experts and platform vendors are promoting the concept of a services model for provisioning data center services and resources to meet changing demands on an as needed basis. There are a number of names being used to describe this model including policy-based computing, utility computing or on-demand computing.

The benefits of this utility computing concept include improved utilization of CPU, storage and networking resources, faster response to changing demands and possibly improved availability achieved by using a standard platform that can be quickly replaced by quickly provisioning a new environment.

An important component of any utility-based computing solution is an intelligent end-to-end network infrastructure that can be managed, shared and securely provisioned to meet the needs of separate application environments simultaneously. Not only do specific network ports need to be dynamically configured to these separate environments, but also the services such as security, content switching and storage networking.

Cisco Data Center Networking solutions are designed to support a utility environment and provide an evolutionary path to meeting customers desire for a services approach to providing data center networking.

The leading shipping utility data center solution today is HP's Utility Data Center (HP-UDC) solution. Cisco is closely collaborating with HP to provide an end-to-end data center networking infrastructure for HP-UDC. Cisco Data Center Networking solution provides an intelligent infrastructure and services that can be provisioned on-demand, dynamically to meet changing needs in the data center.

Cisco Services and Support

Businesses are beginning to understand that data center networks provide a highly available, scalable, secure, and intelligent network foundation for data center operations to dramatically reduce the risks of costly downtime, lost productivity, data corruption or loss, unsatisfied users or a diluted business brand.

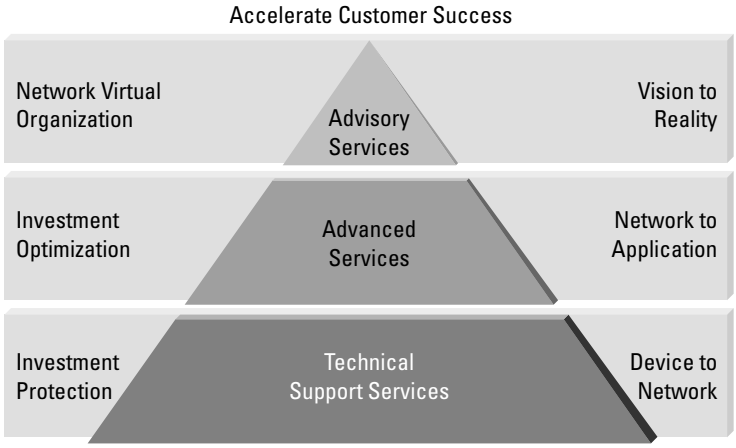
All too often, IT organizations lack the skills required to rapidly and successfully develop the strategies and plans to migrate their existing environment to data center networks. Similarly, in order to realize the significant strategic and operational benefits of data center networks, they need the assistance of experienced and focused engineering support that can optimize network quality of service, availability and security while containing costs. A well-trained, experienced services organization can bridge an IT organization's skills gap.

Cisco experience has shown that customers' networking needs vary, from company to company, and throughout the network life cycle. With this in mind, organizations need options. Cisco has created a flexible and innovative suite of support programs that customers can select individually or in any combination that is right for their network.

Cisco Services Portfolio

The foundation for Cisco Services is a network life-cycle model based on the five basic phases of planning, design, implementation, operation, and optimization. The result is a unique portfolio of complementary service components: Technical Support Services, Advanced Services and Advisory Services. These services span the continuum of device, network, and application support for the Cisco high-performance network, enabling seamless integration, high availability, and nonstop scalability to keep pace with changes in geographical coverage and with business and customer demands. Cisco services can make it happen!

Figure 21
Cisco Services Portfolio



Cisco Technical Support Services

Cisco and Cisco qualified partners provide global, 24 x 7 technical support and technology investment protection that is critical to your data center networking solution operations. Cisco provides Cisco SMARTnet and SMARTnet technical support services. Cisco partners' technical support services are backed by Cisco technical expertise on the data center network devices. Through a structured coordinated support process, integrated network solution issues can be resolved through collaboration with third party product vendors.

Cisco Advanced Services

Cisco and Cisco qualified partners can help you assess, plan, and design a data center networking migration strategy and solution as well as implement and test your data center network. Cisco and its partners may be utilized independently or together to deliver end-to-end data center networking solutions. Cisco and its partners have demonstrated project management skills ensuring consistent delivery of services on demanding projects with a strong customer satisfaction record.

Cisco Advanced Services consists of a unified suite of professional engineering support offerings designed to assist enterprise and service provider customers in realizing business return on investment (ROI) through high performance networking and communications applications enablement. Service components from Cisco's Advanced Services portfolio can be flexibly packaged to meet your unique needs.

Cisco Focused Technical Support: Delivers responsive, rapid problem isolation through personalized attention and special access to engineering resources with expert knowledge of your network and operational processes, driving operational efficiency and enabling you to apply internal technical resources to more critical functions such as network planning.

Cisco Network Optimization Support: Provides expert advice on network design, network capacity planning, configuration management, software migration and network operation for your Cisco routing, switching and optical network infrastructure. This enables you to maintain high performance, availability, and quality of service levels that results in efficient network scalability, efficient introduction of new IP services, improved customer satisfaction, and maximized network return on investment (ROI).

Cisco Technology Application Support: Speeds the introduction of key communications technologies such as storage networking, VPN, wireless LAN, content networking and security via proactive, consultative support. Migration planning, design, implementation and technology optimization planning are enhanced through direct access to Cisco engineering resources and best practices.

Cisco Network Availability Improvement Support: Whether the downtime is a catastrophic network outage or an isolated interruption of service businesses can suffer the loss of revenue, customer satisfaction, and an erosion of customer loyalty. Cisco Network Availability Improvement Support helps you improve your network availability, resiliency, and operational efficiency through availability assessments, benchmarking, and an improvement process that improves network availability and minimizes risks associated with resiliency, operational processes, and network management effectiveness.

Cisco Security Posture Assessment: Identifies the extent of your network's security vulnerabilities, evaluates the effectiveness of current safeguards, and assesses your organization's ability to detect and respond to attack then recommends ways to address vulnerabilities to improve your overall network security.

Cisco Knowledge Transfer and Mentoring: Improves the skills of your staff with innovative and customized knowledge transfer and mentoring services that offer quick, scalable, and cost-effective transference of Cisco networking expertise and best practices.

Leverage Cisco: The Networking Experts

Whether you need to develop a networking strategy for business continuance planning, consolidate storage by implementing a storage area network, or increase availability by enhancing your operational processes, the unmatched experience of Cisco Services and Support can help you realize the full potential of your data center networking efforts.

Summary

An organization's ability to utilize information technology and the Internet to achieve productivity gains, streamline business processes, and improve customer satisfaction is fundamental to a company's short-term and long-term success and profitability. By providing controlled environments for the centralization of critical computing resources, data centers are the key resource for delivering on those short-term and long-term success and profitability goals. However, data centers are also very expensive to develop and maintain. Therefore, many IT organizations are undertaking numerous initiatives to evolve their data center infrastructures to achieve improvements in productivity, while at the same time improving business resilience and higher levels of flexibility and agility.

Cisco Systems, the world leader in networking technologies, teams with IT organizations to achieve their data center productivity and resilience goals through both incremental upgrades to existing networking infrastructure and by providing proven and validated, end-to-end data center networking blueprints for completely new data centers. Cisco data center networking solutions deliver a reliable, secure and application-aware platform that supports optimized user access to applications and services, interconnectivity between server and storage computing resources as well as interconnectivity between data centers. By deploying an optimized network foundation, data center operations drastically reduce the risks of costly downtime, lost productivity, data corruption or loss, unsatisfied users and a diluted brand. Built upon open and standards-based solutions, the flexibility of the Cisco data center network infrastructure allows customers to take advantage of new technologies that increase data center productivity and

efficiency while protecting existing investment, By joining forces with leading infrastructure, application and integration partners. Cisco also provides customers with enhanced data center network solutions for specific environments.

For more information about Cisco Data Center Networking Solutions, visit http://www.cisco.com/go/datacenter.

Related Links

Cisco Data Center Networking—http://www.cisco.com/en/US/netsol/ns110/ns53/net_solution_home.html

Cisco Data Center Networking Reference Design Guidance—
http://www.cisco.com/en/US/netsol/ns110/ns53/ns224/networking_solutions_packages_list.html

Resilient IP Network Infrastructure—http://www.cisco.com/en/US/netsol/ns110/ns146/net_solution_home.html

Integrated Policy-Based Security—http://www.cisco.com/en/US/netsol/ns110/ns170/net_solution_home.html

Application and Server Optimization—http://www.cisco.com/en/US/netsol/ns110/ns49/net_solution_home.html

Storage Networking—http://www.cisco.com/en/US/netsol/ns110/ns258/net_solution_home.html

Operational Efficiency—http://www.cisco.com/en/US/netsol/ns110/ns106/net_solution_home.html

ECOstructure—http://www.eecostructure.com

Microsoft Systems Architecture—
http://www.cisco.com/en/US/partners/pr67/pr41/partners_strategic_solution09186a008014545c.html

HP Utility Data Center—
http://www.cisco.com/en/US/partners/pr67/pr29/partners_strategic_solution09186a00800d79e3.html

Technical Support Resources—http://www.cisco.com/en/US/support/index.html

Networking Professionals Connection—http://forum.cisco.com/eforum/servlet/NetProf?page=main

Glossary

2-Tier Architecture—Some of the earlier mission-critical client-server applications such as ERP used a two-tier architecture in which application processing is split into two parts between the client workstation and the server. The client runs the presentation and the majority of the application logic. The server stores the information on a database and also runs some application logic. This is often referred to as “fat client” architecture.

3- Tier Architecture—In a 3-tier model, the presentation, application, and the database all reside on separate computers. In the 3-tier architecture, application logic is detached from the actual database, allowing for specialized application servers to be deployed using a standard interface to database servers. Since the database servers are a separate entity, they can become a shared resource among multiple applications. This model increases both manageability and portability of both the application and database tiers.

N-Tier Architecture—A true n-tiered web architecture separates user interface, logic, and data into four clearly delineated logical layers: physical UI rendering, logical UI definition, business logic, and data access. An n-tiered architecture provides customers with a broad variety of deployment options with UI, logic, and data being distributed amongst multiple physical tiers.

Authentication, Authorization, and Accounting (AAA)—is a term for a framework for intelligently controlling access to computer resources, enforcing policies, auditing usage, and providing the information necessary to bill for services. These combined processes are considered important for effective network management and security.

Dense wave division multiplexing (DWDM)—Wave division multiplexing (WDM) refers to an optical transmission technique where multiple optical signals are transmitted on a single optical fiber using different wavelengths. The term dense wave division multiplexing (DWDM) is often used to describe systems supporting a large number of channels, with "large" not clearly defined, but ranging from upwards of 16.

DMZ—In computer networks, a DMZ (demilitarized zone) is a computer host or small network inserted as a "neutral zone" between a company's private network and the outside public network. It prevents outside users from getting direct access to a server that has company data.

Dynamic Host Configuration Protocol (DHCP)—is a communications protocol that lets network administrators manage centrally and automate the assignment of Internet Protocol (IP) addresses in an organization's network. Using the Internet Protocol, each machine that can connect to the Internet needs a unique IP address.

Dynamic Naming Server (DNS)—the way that Internet domain names are located and translated into Internet Protocol addresses. A domain name is a meaningful and easy-to-remember "handle" for an Internet address.

ESCON—-(Enterprise Systems Connection) IBM's fiber optic serial channel for attaching mainframes to peripherals such as storage devices, backup units, and network interfaces. This channel incorporates fiber channel technology. The ESCON channel replaces the bus-and-tag channel.

FCP—Fibre Channel is the established layer 2 SAN protocol. It provides robust 1 and 2 Gbps switched connectivity between high-end servers and storage.

FCIP—FCIP supports Fibre Channel communication over an IP network, enabling the interconnection of FC SANs, typically for replication between storage systems over a wide area network

FICON—(for Fiber Connectivity) is a high-speed input/output (I/O) interface for mainframe computer connections to storage devices. As part of IBM's S/390 server, FICON channels increase I/O capacity through the combination of a new architecture and faster physical link rates to make them up to eight times as efficient as ESCON (Enterprise System Connection), IBM's previous fiber optic channel standard.

Firewall Load Balancing (FWLB)—For scalable firewall security, Cisco intelligently directs traffic across multiple firewalls, eliminating performance bottlenecks and single points of failure. Firewall load balancing eliminates system downtime that results when a firewall fails or becomes overloaded—breaking Internet connections and disrupting e-commerce purchases or other mission-critical transactions.

Hot Standby Routing Protocol (HSRP)—A protocol that provides high network availability and transparent network topology changes. HSRP creates a Hot Standby router group with a lead router that services all packets sent to the Hot Standby address. The lead router is monitored by other routers in the group, and if it fails, one of these standby routers inherits the lead position and the Hot Standby group address.

HTTPS—(Hypertext Transfer Protocol over Secure Socket Layer, or HTTP over SSL) is a Web protocol developed by Netscape and built into its browser that encrypts and decrypts user page requests as well as the pages that are returned by the Web server.

ISCSI—Enables servers and storage devices to communicate over IP and Ethernet networks. This technology is complementary to the Fibre Channel Protocol (FCP)

Lightweight Directory Application Protocol (LDAP)—is a software protocol for enabling anyone to locate organizations, individuals, and other resources such as files and devices in a network, whether on the public Internet or on a corporate intranet.

Network Attached Storage (NAS)—File-oriented storage networking implementation, deployed in the form of customized storage appliances that are connected to the IP network. Due to the file abstraction layer, NAS offers both storage and data sharing services across multiple platforms and protocols.

Secure Sockets Layer (SSL)—A security protocol that provides communications privacy over the Internet. The protocol allows client/server applications to communicate in a way that is designed to prevent eavesdropping, tampering, or message forgery.

SONET—is the American National Standards Institute standard for synchronous data transmission on optical media. The international equivalent of SONET is synchronous digital hierarchy (SDH). Together, they ensure standards so that digital networks can interconnect internationally and that existing conventional transmission systems can take advantage of optical media through tributary attachments.

Storage Area Network (SAN)—The term Storage Area Network defines the hardware and software associated with enabling block-level data transfer between storage devices and hosts in a networked paradigm. Today, the predominant SAN technology is Fibre Channel, however with the creation of iSCSI, we can expect a combination of FC and technologies to form the infrastructure for SANs in the future.

SNA—SNA is a proprietary IBM architecture and set of implementing products for network computing within an enterprise. It existed prior to and became part of IBM's Systems Application Architecture (SAA) and it is currently part of IBM's Open Blueprint. With the advent of multi-enterprise network computing, the Internet, and the de facto open network architecture of TCP/IP, IBM is finding ways to combine its own SNA within the enterprise with TCP/IP for applications in the larger network.

Synchronous Disk Mirroring—A method of ensuring that identical data is stored on separate storage media in real time, typically for purposes of protecting against disk failure or where remote mirroring is implemented, for disaster recovery.

Virtual LANs (VLANs)—is a local area network with a definition that maps workstations on some other basis than geographic location (for example, by department, type of user, or primary application).

Virtual Private Networking (VPN)—is a way to use a public telecommunication infrastructure, such as the Internet, to provide remote offices or individual users with secure access to their organization's network.

VTAM—(Virtual Telecommunications Access Method) is an IBM application program interface (API) for communicating with telecommunication devices and their users. VTAM was the first IBM program to allow programmers to deal with devices as "logical units" without having to understand the details of line protocol and device operation. Prior to VTAM, programmers used IBM's Basic Telecommunications Access Method (BTAM) to communicate with devices that used the binary synchronous (BSC) and start-stop line protocols.

XML—Extensible Markup Language—A language that allows developers to create customizable tags to aid in the definition, transmission, validation, and interpretation of data between applications.

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.
Capital Tower
168 Robinson Road
#22-01 to #29-01
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 Web site at www.cisco.com/go/offices

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica • Croatia 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

DB/LW4225 02/03