

# Cisco AVVID Solution

A decorative graphic on the left side of the page, consisting of a blue square with a white grid pattern, partially overlapping a black vertical line that extends from the top of the page down to the bottom.

## AVVID Common Infrastructure : Storage Networking



## Introduction

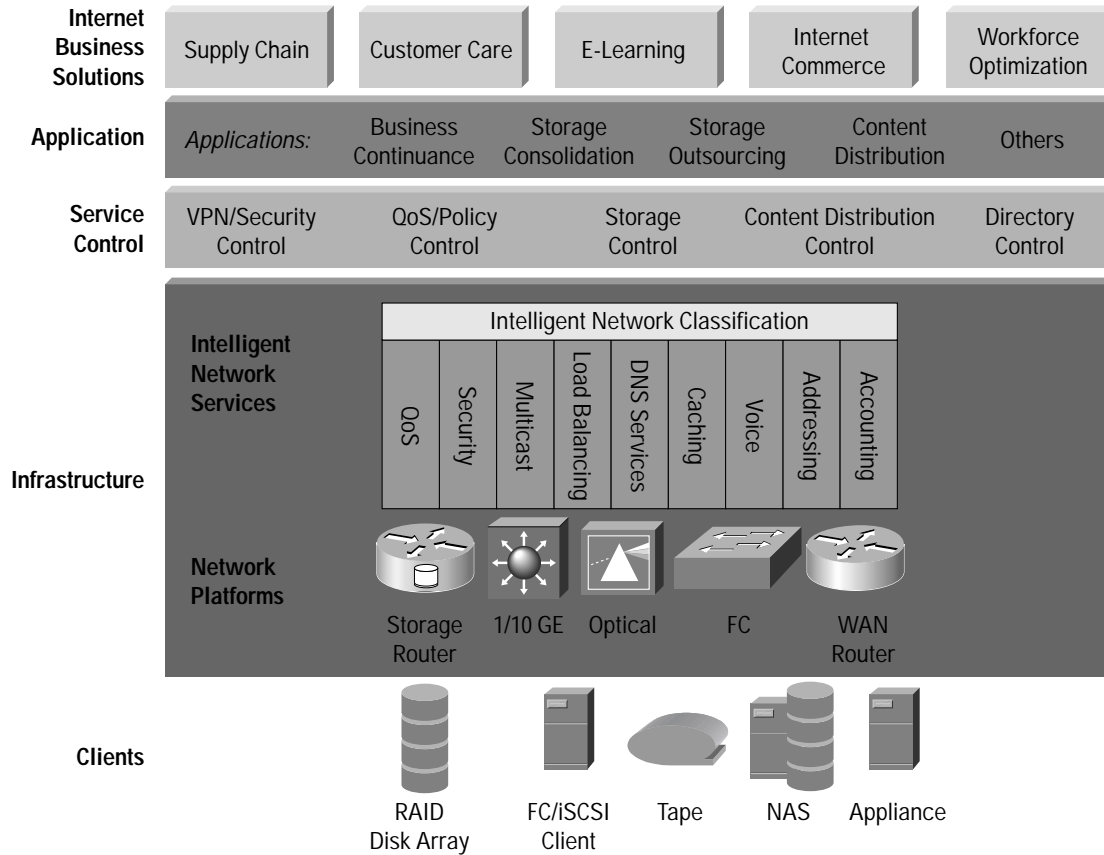
Cisco AVVID (Architecture for Voice, Video, and Integrated Data) is a standards-based open systems architecture for multiservice or converged enterprise networks. Cisco AVVID is based on the AVVID Common Infrastructure, which forms the foundation for converged IP-enabled enterprise networks. Cisco Systems is also developing common infrastructure best practices to provide customers with well-defined and verified guidelines for the deployment of the Cisco AVVID storage networking solution within a converged IP network, such as Cisco AVVID Common Infrastructure.

This paper shows how the current storage paradigms are changing as Fibre Channel (FC) and IP networks converge toward an integrated storage networking infrastructure, such as Cisco AVVID storage networking. This eliminates the limitations of separate storage-area network (SAN) islands. The convergence of storage and network enables the Cisco AVVID storage networking solution to integrate the technology already deployed in IP networks with new standards, protocols, and products, such as Small Computer Systems Interface over IP (iSCSI), the storage router, and the Fibre Channel IP (FCIP) protocol. Cisco storage networking solutions address a variety of technologies and product approaches that facilitate access and interconnection of storage to form a storage utility pool that is managed across the global enterprise. The core networking technology enablers are IP, Gigabit Ethernet, Fibre Channel and optical networking, which provide universal access and interconnection for Network-Attached Storage (NAS) and SAN environments. Cisco strategy is based on an open architecture that leverages intelligent IP, Gigabit Ethernet, Fibre Channel and optical networking technologies combined with industry-leading partner solutions to enable scalable, cost-effective universal access and management of storage information. Anticipating the customer challenges and technology trends, Cisco addresses customers' plans to extend networked storage beyond the data center, taking advantage of technologies that are predominant not only in the data center, but also in MAN and WAN environments.

## Cisco AVVID Infrastructure for Storage Networking

Cisco views the storage network as another component of the Cisco AVVID Common Infrastructure, which supports converged data, voice, and video applications. Figure 1 shows how the storage networking solution is integrated with the Cisco AVVID Common Infrastructure.

**Figure 1** Cisco AVVID Building Block for Storage Networking

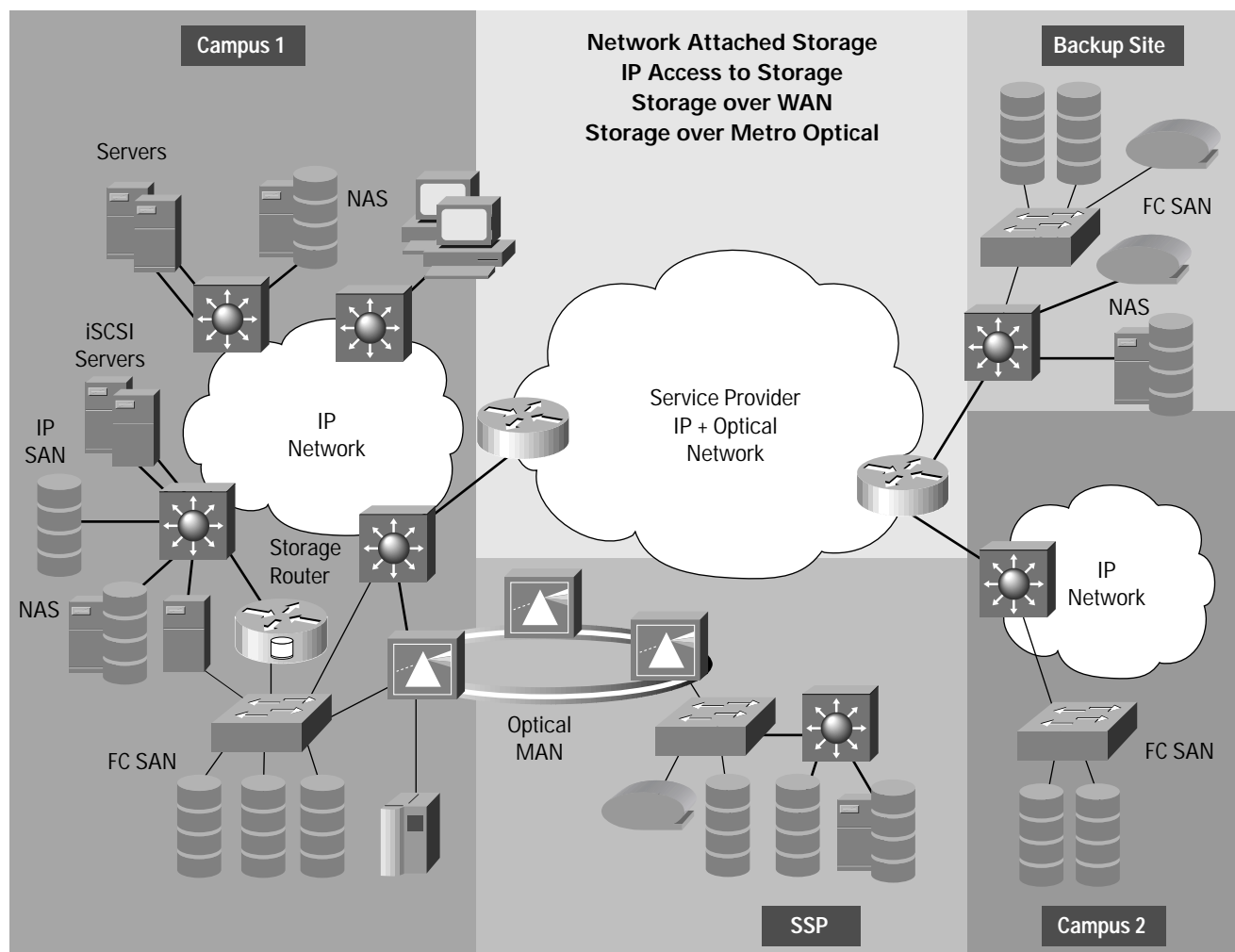


**Storage Networking Architecture**

The following figure shows the deployment of the Storage Networking architecture throughout the Cisco AVVID Common Infrastructure.



Figure 2 Storage Networking Architecture



Key components of the storage networking solution are the following:

- Network-attached storage for file-oriented access to storage
- Universal IP access to storage for block-oriented host-to-storage communication
- Storage over the WAN, for the interconnection of all storage environments
- Metro optical connectivity for the efficient, high-performance transport of storage traffic types, including Fibre Channel, 1/10 Gigabit Ethernet, and Enterprise System Connection (ESCON).

Storage networking is the hardware and software that enables storage to be consolidated, shared, and accessed over a networked infrastructure. Cisco AVVID Common Infrastructure provides a storage networking architecture that extends beyond the data center, across the campus, the metro and the wide area. Cisco AVVID Common Infrastructure supports both SAN and NAS storage networking models, treating them as complementary technologies that simultaneously use the Cisco AVVID Common Infrastructure:

- SAN provides block-oriented access to native disk storage. It is based on a shared or switched Fibre Channel infrastructure; however, SAN can now also be extended to an IP infrastructure. New protocols and products are emerging that allow the integration of Fibre Channel SANs with the IP network. This paper discusses two protocols supported by Cisco: iSCSI and FCIP. Historically, SANs have been well suited to high-performance, write-intensive database applications.
- NAS provides file-oriented access over an IP network. NAS filers are customized storage appliances that run Network File System (NFS) for UNIX environments and Common Internet File System (CIFS) for Microsoft Windows NT and Microsoft Windows 2000 environments. NAS is deployed in high performance file-sharing applications for engineering collaboration, NT file systems, e-mail, and Web content storage.

Most enterprises deploy a combination of NAS and SAN strategies to meet the wide range of application environments. Differentiation between these technologies will disappear as storage architectures converge to provide both file and block-based services.

### Storage Networking Applications

The key storage networking applications can share, access, and manage information resources efficiently. The following sections discuss two storage networking applications: storage consolidation, and business continuance applications such as disaster recovery, and backup and restore applications.

#### Storage Consolidation

Many enterprises have already implemented storage networking SAN or NAS architectures and want to leverage the existing infrastructure to consolidate storage. With the rapid growth of digital information, the amount of data and servers has also increased. System administrators are faced with the challenging task of managing storage and making it scalable to accommodate future needs. With storage directly attached to the server, scalability is difficult. The storage expansion capability is limited to the capacity of the server (for example, as measured by the number of I/O controllers and devices per controller that can be configured in the server). Because of the nature of the SCSI bus that is traditionally used to connect disks to a server, it is difficult to allocate more disk storage without interrupting and rebooting the server, and thus affecting applications.

To accommodate growth, rapid deployment of additional storage must have minimum or no impact on the applications' availability. Rapid and simplified scalability is created by a pool of disks attached to the network which provide servers universal file or block access to the storage.

The addition of servers and storage resources to accommodate rapid growth results in a more difficult environment to manage, with poor use of resources. A best practice approach is to provide all servers that do not have access to the SAN with IP access to the storage and allocate storage on demand. This storage consolidation provides centralization and simplification of storage management.

#### Disaster Recovery

Today's storage and networking architectures do not tolerate any interruption of operation, and enterprises are forced to implement stringent disaster recovery plans to guarantee the recovery of services in a timely and cost-effective manner. Customer enterprise-wide information is protected according to its level of criticality, the length of time required to recover the information, and whether the potential loss in information is acceptable.

A higher level of information is achieved through mirror sites: a complete replicated storage, server, network, and application infrastructure in two remote locations. The information is synchronously replicated, in real time, between the mirror sites.



Lower levels of protection include asynchronous mirroring: The information is replicated in an asynchronous manner at a selected frequency. In this asynchronous mode of replication, snapshots, or point-in-time copies of the data, are taken and transferred to a remote site. The point-in-time image is used for disaster recovery, but could potentially be used to perform tasks that must be accomplished on architecture independent of the production site (for example, data mining, reporting, backup).

### Backup and Restore

Disaster recovery applications, such as mirroring and replication, protect against equipment or site failures to provide a highly available infrastructure. However, they do not protect against user errors or data corruption. Backup and restore is the best protection against any kind of data loss. Tapes are also used for permanent off-site archiving for long-term protection of key information for future reference or audit purposes. With the rapid growth of data the amount of backups required has increased, yet the timeframe allowed for backup is limited. Backups impact the performance of the server, and management of backups has become increasingly more complex as the amount of information grows.

Backup has evolved from an architecture in which tape drives were directly attached to the server. Now the network backup uses tape drives attached to a centralized backup server or to a SAN-based, networked tape library. When storage area networks first emerged, tape autoloader or tape libraries constituted a consolidated backup system. Snapshot technology now makes it possible to back up systems online with minimum impact on the applications.

### Storage Networking Convergence

Until today, block access has been associated with Fibre Channel SANs, and file access with NAS. However, this paradigm is changing as Fibre Channel and IP networks converge toward an integrated storage networking architecture. Cisco sees storage networks as an infrastructure that enables file and block access over interconnected FC and IP networks. Cisco supports the development of new protocols that allow the convergence of Fibre Channel with Corporate IP networks.

Figure 3 Conceptual View of Today's Storage Networking Architecture

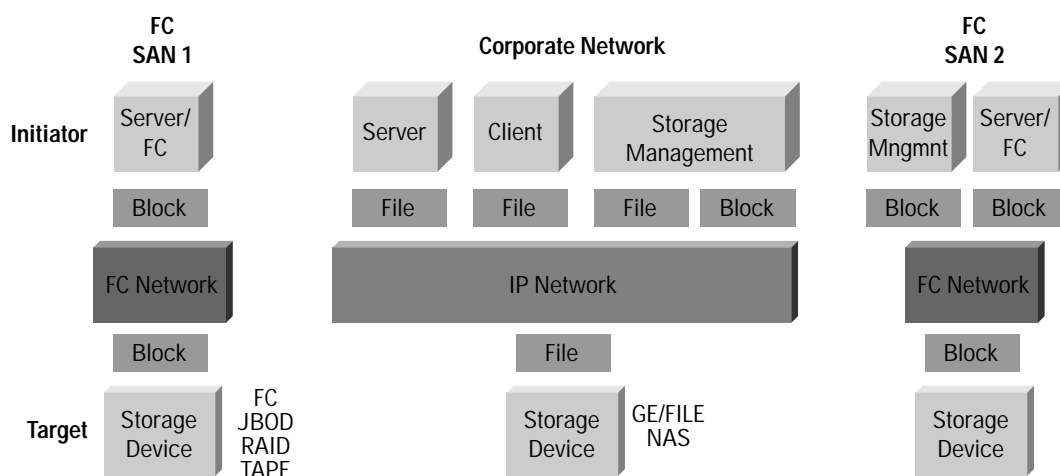


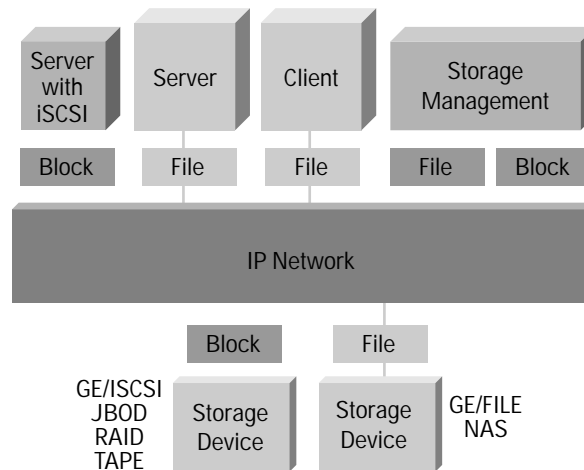
Figure 3 describes a conceptual view of today's storage networking architecture. The IP network, based on open standards, provides file access to storage. Storage Management, along with device administration, provides services such as storage virtualization or the pooling of storage capacity from mixed vendor environments. Clients and servers are the two components involved in file system sharing in a NAS environment. Clients, for example, can be workstations, which are given access to files on a NAS device.

Initiators and targets in the FC SAN participate in the establishment of a SCSI session. The initiator, or client, requests data on the storage device, the target.

Storage area networks form isolated islands that are difficult to interconnect. The storage networking solution integrates the corporate IP network with the FC network islands by providing either IP access Network Attached Storage for file access or storage area network for block access (iSCSI) over the LAN, WAN, and metro optical. The sections below describe these four components of the solution.

### Network-Attached Storage—File Access to Storage

Figure 4 File Access to the Storage—NAS



Network-attached storage devices use the IP infrastructure to deliver file access to a number of clients, workstations, or servers connected to the IP network. One of the major benefits of NAS is its ability to do scalable and high performance file-sharing for engineering collaboration, NT file systems, e-mail, and Web content storage. Additional benefits of NAS devices include: low cost of ownership, quick and easy storage scaling without impact on a host server, use on existing LAN infrastructure and relief for servers from performance that impacts file management.

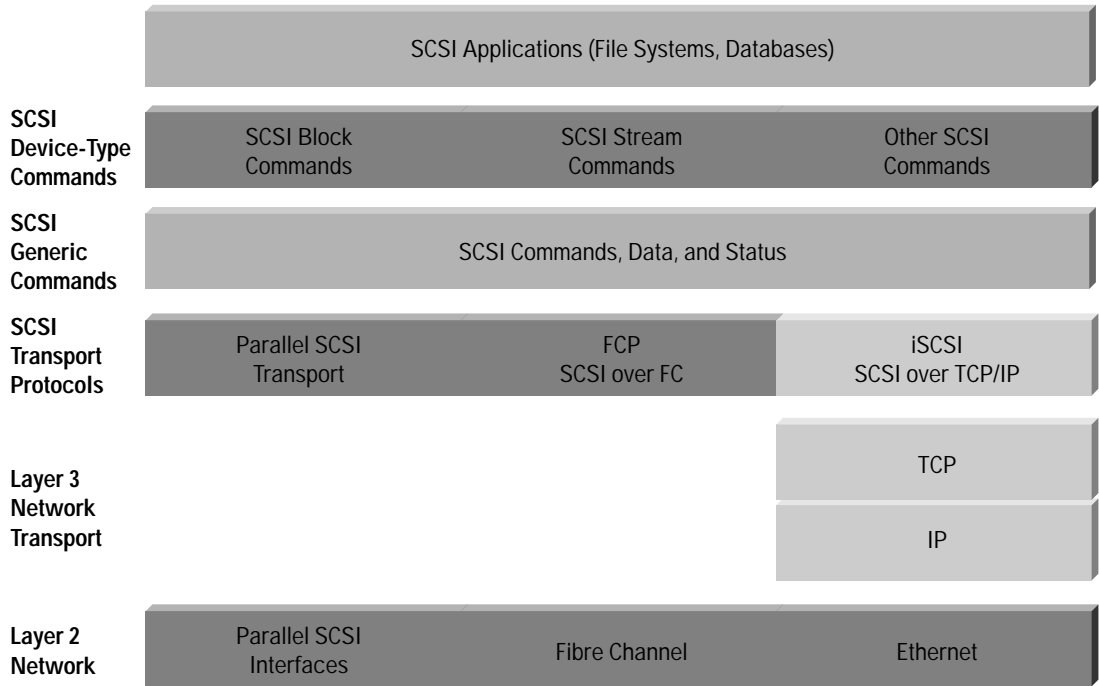
The IP network infrastructure uses open standards that allow ubiquitous and interoperable access to files. It runs at Gigabit speeds with Gigabit Ethernet and, in the near future, 10-Gigabit Ethernet. Today the processing associated with the TCP/IP stack in servers is performed by the operating system. It is software-based and consumes CPU cycles on the server. In the future, TCP/IP processing will be done in hardware and will enable high-speed block access transfers over IP network. Several network interface card (NIC) vendors are addressing this requirement, and new NIC cards that process the TCP/IP stack will be available later in 2001.

### IP Access to Storage— iSCSI

Applications that are I/O intensive and that require high bandwidth have been particularly well suited for block-oriented access. Storage area networks have been primarily built around these types of mission-critical database applications, and fibre channel fabrics have delivered the high throughput that these applications demanded. The gigabit speed of FC, coupled with the processing of the network stack in hardware and larger packet sizes, enables higher performance in the transfer of blocks of data for database applications. This is accomplished at distances ranging up to 10 kilometers without extension.



**Figure 5** iSCSI Allows SCSI Data and Commands to Run Transparently over a TCP/IP Network



Cisco is actively participating in the standardization of iSCSI (SCSI over IP) to enable block access to storage over an IP infrastructure. iSCSI is a draft standard that is undergoing ratification by the IETF IP Storage working group. iSCSI enables servers to communicate with storage over the IP infrastructure. iSCSI encapsulates the SCSI command set and data frames into TCP/IP and is therefore transparent to the application.

**Figure 6** iSCSI Enables IP-Attached Clients to Access Block-Level Storage

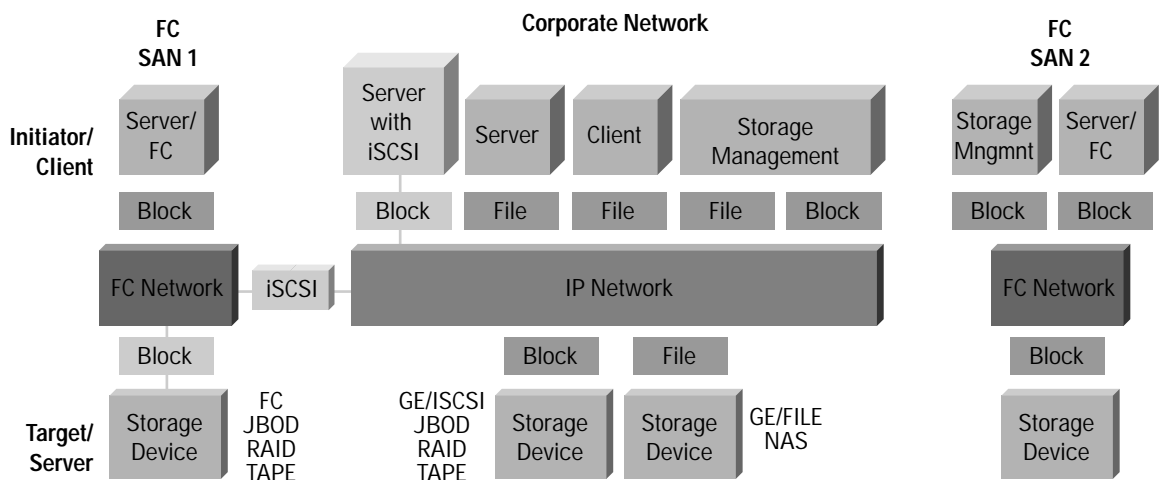


Figure 6 shows how block accesses to storage are made through the interconnected IP and FC network. Through the iSCSI device driver, the server is able to access Logical Units, or volumes, that reside on the Fibre Channel connected storage. The storage router acts as a bridge between Fibre Channel and the IP network. One or more TCP sessions support the communication between the SCSI initiator and SCSI targets. The key technologies that enable the transfer of blocks of data over the IP network are:

- iSCSI routers enable connection of iSCSI hosts to Fibre Channel connected storage. Along with the iSCSI router, iSCSI device drivers provide the interface between the operating system and the TCP/IP stack.
- Gigabit Ethernet provides the bandwidth necessary for the transfer of I/O intensive data.
- Network Interface Cards process the TCP/IP stack. The processing of the TCP/IP stack in the NIC reduces CPU load on the servers.

Figure 7 Block Access to the Storage with iSCSI

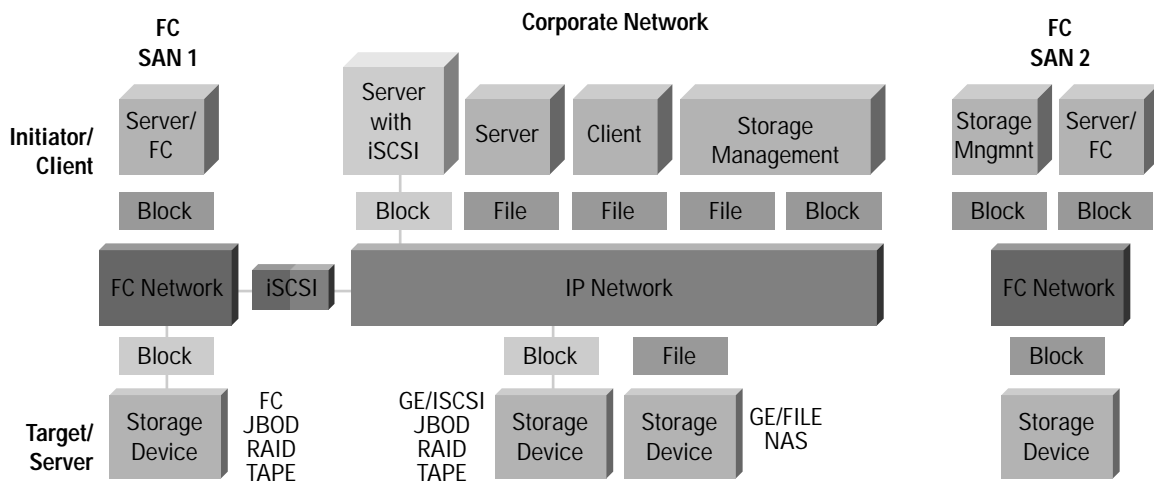


Figure 7 shows how storage devices use iSCSI to provide block access to servers through the high-speed, Ethernet network. Most likely, enterprises that already have a consolidated Storage Area Network prefer to leverage their centralized pool of storage and use an iSCSI router to access the SAN Island. iSCSI technology with Gigabit Ethernet enables the emergence of storage appliances or devices connected to the IP network. iSCSI is an open-based standard providing interoperability and using the existing high-speed, Ethernet infrastructure.

#### Converged Storage Networking Application—Storage Consolidation Using iSCSI

Few servers have access to the Storage Area Network. Only servers that support mission critical applications within the data center have access to SAN. Many servers, however, still have direct attached storage and are subject to high growth of storage utilization. At the same time, enterprises want to best use and leverage the consolidated pools of storage created with storage area networks.

Servers that have direct attached storage and need block access to the storage can use iSCSI and the storage router to allocate storage from the enterprise storage pool. Once IP access to the storage is established, any server can allocate storage through configuration of the Cisco storage router SN5420. Servers are not required to install additional hardware; they simply install a software driver that is supported by major operating systems.



The network design and deployment strategy for iSCSI depends on the existing network architecture, as well as the application performance and security requirements. The storage traffic can be deployed across the same network as the other enterprise applications, or alternatively on a network that is either logically (virtual LAN [VLAN] or virtual private network [VPN]) or physically separate from the enterprise network. In either case, the benefits of using a common technology; management tools, and advanced IP services such as quality of service (QoS), security, and high availability, are clear.

## Storage over the WAN

### Proprietary Storage over IP Solution

The ability to interconnect isolated fibre-channel SANs over an IP network has been limited and based on proprietary technologies.

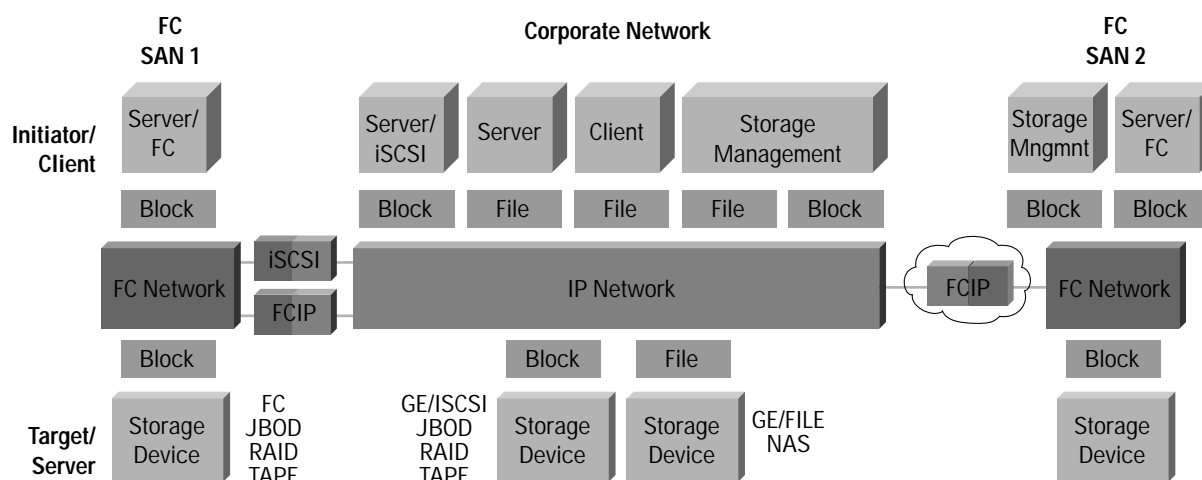
As an example, SRDF-over-IP from EMC uses CNT converters for bridging Fibre Channel and IP. SRDF is a business continuity solution that allows data replication for EMC Symmetrix volumes between geographically dispersed sites. For sites with a distance beyond the metropolitan environment (about 100 kilometers), it is possible to use a WAN for the asynchronous replication of data. Traditionally, a converter of ESCON or Fibre Channel to IP is required for the transfer of storage over the WAN. The SRDF traffic encapsulated into IP frames is then carried over the WAN.

### FCIP

With the goal of achieving open standards-based way of interconnecting Fibre Channel SAN islands, the storage and networking industries are cooperating to develop a standard called Fibre Channel over IP (FCIP).

FCIP is a protocol that is being drafted in the IETF. FCIP relies on the IP network to provide the connectivity between the SAN islands over the WAN, and TCP to provide reliable delivery. With FCIP, Fibre Channel frames are encapsulated within IP packets. FCIP creates a tunnel between two devices connected to the IP network, enabling the interconnection of two point-to-point, storage-area network islands.

Figure 8 FCIP Provides Transparent Interconnectivity of SAN Islands



FCIP differs from iSCSI as follows:

- iSCSI encapsulates SCSI commands and data in a TCP/IP packet. In this case, an IP-connected host running an iSCSI driver is accessing block-level data over an IP network.
- FCIP encapsulates Fibre Channel in IP packets. In this case, any Fibre Channel packet, SCSI/FCP or otherwise, is transported transparently in an IP packet. FC hosts and storage communicate on both sides of an FCIP link.

The FCIP devices are responsible for mapping Fibre Channel fabric domains to IP addresses. Some enterprises are looking for global interconnection between their remote data centers. FCIP provides connection of SAN islands over the WAN—connections that were not previously possible—allowing centralized management of the storage and global access.

FCIP extends storage area networks over the WAN and provides peer-to-peer connection between SANs. With FCIP, enterprises optimize the use of their existing WAN infrastructure. Remote data replication, or backup, is performed when use of the WAN is low. Asynchronous data replication, or backup applications, require high bandwidth but are less sensitive to latency. A response time of a few milliseconds is acceptable for backup or asynchronous replication applications.

#### Converged Storage Networking Application—Remote Mirroring

Replication of data across the WAN has many applications. For enterprises that have multiple data centers in remote locations, the WAN represents a link that can be potentially leveraged for mirroring data asynchronously. An OC-3 link, for example, delivers a bandwidth of 15 MB per second, which is equivalent to the throughput of ESCON. The data replicated is used for data mining, reporting, or disaster recovery. With FCIP, enterprises optimize their existing WAN infrastructure by deploying remote data replication, or remote backup.

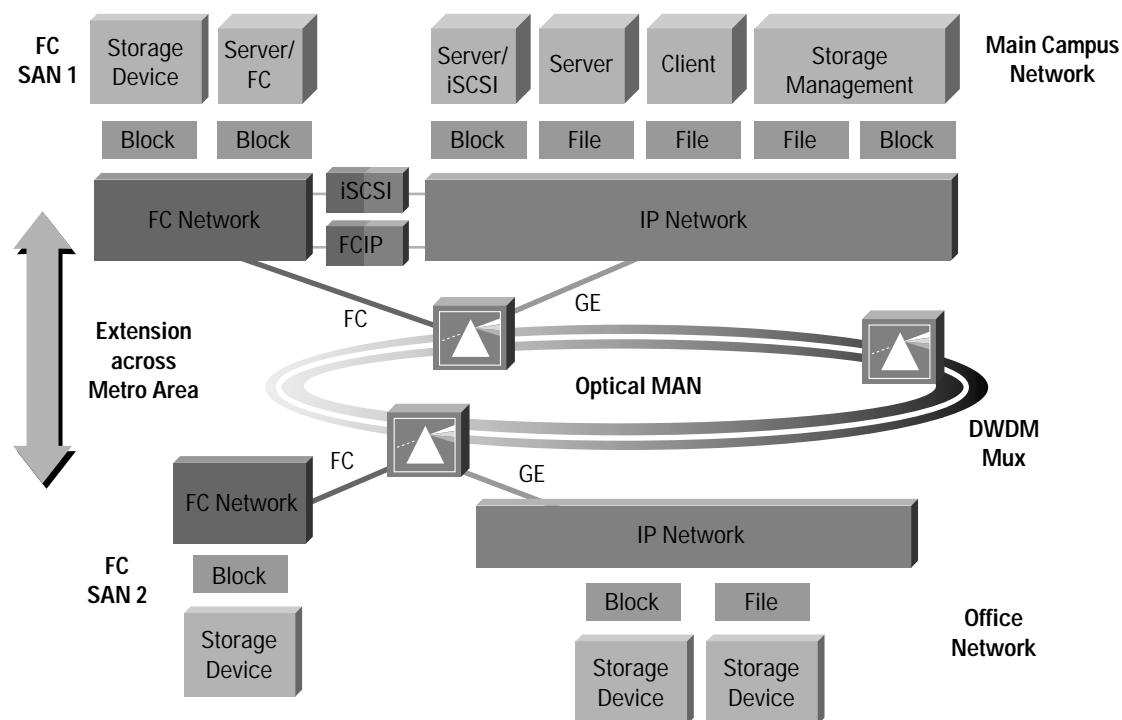
Data backup consists of copying the data to local or remote tape to protect it from corruption or loss. Once the data is on tape, it is important to regularly send the tape to a remote site or vault to efficiently protect the information against a major site disaster. FCIP enables the backup of data between geographically remote locations through the WAN. FCIP is completely transparent to the application; the remote tape is seen as if it is attached to the local SAN. Restoring from an offsite tape is simplified and accelerated, reducing costs and delays.

#### Metro Optical—DWDM

Optical fiber is deployed in many metropolitan areas at a rapid rate, leading to increased fiber availability and lower leasing costs. Dense wavelength-division multiplexing (DWDM) allows for a transparent multiplexing of voice, video, or data traffics over the same physical fiber optic link. By using the properties of DWDM, both IP-based and Fibre Channel-based storage networks are extended transparently across the metropolitan area, as shown in Figure 9.



**Figure 9** Extension of NAS and SAN Environments across the Metropolitan Area Using DWDM Technologies



The DWDM infrastructure is used for both storage-to-storage traffic and host-to-storage traffic, whether NAS- or SAN-based. By using different wavelengths, DWDM allows multiple optical channels, each operating at multigigabit speeds, to travel over the same optical fiber. With only a few wavelengths, enterprises scale bandwidth dramatically. Enterprises connect remote sites across fiber at high speed, making the access between users and network data storage seamless. Because of its transparency, DWDM is uniquely matched to meet the high bandwidth and low latency requirements for storage, especially for the most latency-sensitive applications, such as storage I/O or synchronous mirroring.

#### Network Services for Storage Networking

IP-based storage technology has been developed for many years by the networking industry. The services that exist today in IP networks provide a firm base to use in achieving universal, secure, and robust deployment of storage networking applications. These services include availability, QoS, security, load balancing, and management.

#### Availability

High availability for storage networking solutions means data everywhere anytime. Access to strategic information must be maintained without interruption. High availability is achieved through a network infrastructure designed for fault resiliency and storage solutions that are highly reliable and protected against failure. Cisco switches and routers have advanced redundancy and high availability features. The Cisco IOS Software<sup>®</sup> also provides several high availability features. Hot Standby Routing Protocol (HSRP) provides a mechanism for ensuring the availability of routing services from a pool of router resources. HSRP uses a standby router from the pool in case the primary router device fails. If a failure occurs on a device, all traffic is directed to another router in the HSRP pool.

The Cisco IOS Software also supports a full complement of robust network routing protocols, such as Open Shortest Path First (OSPF), Border Gateway Protocol (BGP), and Enhanced Interior Gateway Routing Protocol (EIGRP). These protocols can route traffic through the network using the most efficient path. If the best path becomes unavailable, these routing protocols automatically choose the next best path for the traffic to ensure it reaches its destination. These IOS routing protocols are deployed in the WAN to ensure a reliable and efficient path for the IP traffic.

## Security

The Cisco SAFE blueprint for security is a flexible, dynamic, security blueprint for networks that is based on Cisco AVVID. Cisco SAFE secures e-business using a modular approach to simplify security design, rollout, and management. The Cisco SAFE blueprint addresses the entire enterprise, including the switched backbone or core, central server farm, the building distribution layer, the wiring closets, and central management services. Beyond the campus, the edge distribution layer connects the corporate network to the outside world through Internet access, remote-access VPNs, private WAN lines, and e-commerce. Each of these modules has a unique SAFE design which may include firewalls, intrusion detection and scanning systems, device and user authentication, antivirus technologies, encryption, tunneling, and VPN concentrators.

As networking takes a prominent place within storage architecture, these security modules and designs are essential in deploying secure storage solutions.

- VPNs are used to secure end-to-end private networks over a public infrastructure. Site-to-site VPNs use tunneling and encryption technology for data privacy.
- Firewalls enforce the security policy and restrict access to the network infrastructure. Intrusion detection systems detect unauthorized access, terminate these network sessions, and log the events.
- Authentication is performed through access control servers that validate user identities.
- Security managers are used to deploy security policies and rules.
- Private VLANs provide some added security to specific network applications. Private VLANs work by limiting which ports within a VLAN communicate with other ports in the same VLAN. This effectively mitigates the effects of a single compromised host.

## Quality of Service

Quality-of-service (QoS) features define the delivery terms for a particular traffic flow. Establishing QoS delivery terms ensures that the specified traffic is given priority over other, less-important traffic—when dealing with time-sensitive or mission-critical traffic. To apply QoS mechanisms, the traffic must be classified and marked with a user-defined Differentiated Services Code Point (DSCP).

The class of service (CoS) defines the priority of the traffic flow. Classification of the traffic is accomplished through Access Control List (ACL). Traffic flow with a specific packet header information, IP addresses of the source or destination, and port number are easily identified with ACLs. For example, iSCSI storage traffic uses well-known TCP port number 5003 and can be marked with a DiffServ code point that is treated with a higher priority.

Other Cisco IOS Software features ensure that important traffic is delivered efficiently: traffic shaping and low latency queuing. Cisco switches allow the aggregation of Ethernet ports to create a channel. The aggregated port is called EtherChannel. EtherChannel, composed of multiple Gigabit Ethernet links, can load balance traffic across those links. Unicast, broadcast, and multicast traffic is evenly distributed across the links providing higher performance and redundant parallel paths. If a link failure occurs, traffic is redirected to remaining links within the channel without user intervention in less than a few milliseconds. This convergence is transparent to the end user.

The channel provides automatic recovery for loss of a link by redistributing loads across remaining links. When the failed link comes back up and joins the EtherChannel, it remains transparent to the end user. As the EtherChannel works at Layer 2, all the above Layer protocols are supported.



The Cisco EtherChannel implementation supports load balancing based on source and destination IP address, Layer 4 port numbers, and standard source and destination MAC address. This gives flexibility to the customer in load balancing, depending on the specific requirements.

EtherChannel is used in NAS environment providing scalability to the bandwidth. NAS have multiple Gigabit Ethernet interfaces per device.

### **Network Management**

The management of enterprise IP network is defined in four areas: LAN, WAN, service level, and security management. In these four areas, solutions exist to manage the network and devices in an end-to-end perspective. CiscoWorks2000 is a family of products that provides solutions targeted at the wide-area and local-area operations of enterprise networks.

CiscoWorks2000 provides management in these four areas as follows:

- LAN management—provides operationally focused applications for configuration, fault monitoring, and troubleshooting campus networks.
- Routed WAN management—configures, administers, monitors, and troubleshoots routed WANs, dramatically reducing their complexity. This suite of solution applications provides increased visibility into network behavior and quickly identifies performance bottlenecks and long-term performance trends. It also provides sophisticated configuration tools to optimize bandwidth and use across expensive and critical WAN links in the network.
- Service management—implements end-to-end SLAs, enabling ISPs to differentiate their services from competitors and the enterprise to confirm that the ISPs are delivering the agreed level of service.
- Security and VPN management—Cisco Secure Policy Manager, formerly known as Cisco Security Manager, is a scalable, powerful security policy management system for Cisco firewalls and Virtual Private Network (VPN) gateways. With Cisco Secure Policy Manager, Cisco customers can define, distribute, enforce, and audit network-wide security policies from a central location.

### **Conclusion**

This paper described how the current storage paradigms are evolving to converge toward an integrated storage networking infrastructure. The vision for Cisco Storage Networking is to provide company-wide access to a centrally managed global storage based on open architecture and industry standards. The Cisco AVVID Common Infrastructure provides the foundation for achieving this vision. The intelligent network services that are delivered by a Common Infrastructure can be leveraged by storage networking applications such as storage consolidation, disaster recovery and backup. By helping to accelerate the convergence of storage and network technologies, Cisco is bringing the benefits of open, standards-based technologies to the emerging storage solutions of today

### **Annexes**

#### **Enabling Technologies**

The business requirements for networked storage coincide with a number of technological developments that are facilitating the creation of high performance, reliable and scalable storage network infrastructures required by demanding storage applications. These technologies include optical DWDM, IP network services (QoS and security), SCSI over IP (iSCSI), encapsulated FC (FCIP). The following terms are a few of the more prominent technology advances:

**Optical DWDM Technology:** The development of Dense Wave Division Multiplexing (DWDM) optical technologies for the metro or campus area, that allow the transparent transport of 32 or 64 parallel high speed data streams, each of 2.5-10Gbps, on a single fiber are revolutionizing the types of storage applications that can be extended across campus and metropolitan area networks.

IP Services: The acceleration of IP services is resulting in the ability to leverage the huge and ongoing investments that have been made in IP technologies to provide quality of service, provisioning, security and management functionality for storage networks.

iSCSI (SCSI over TCP/IP): iSCSI is a draft standard, awaiting ratification in the IETF's IP Storage working group. It allows multiple servers to communicate with storage over a standard high speed IP infrastructure in a multi-point configuration. iSCSI uses the same command set and data frame as SCSI that rides on a SCSI bus or Fibre Channel, and is therefore transparent to the application.

FCIP (Fibre Channel over IP): FCIP is a second draft standard awaiting ratification in the IETF IP Storage working group. It is complementary to iSCSI and enables inter-connection of Fibre Channel SAN islands over an IP MAN/WAN infrastructure in a point-to-point configuration.



**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 Europe  
11, Rue Camille Desmoulins  
92782 Issy Les Moulineaux  
Cedex 9  
France  
www.cisco.com  
Tel: 33 1 58 04 60 00  
Fax: 33 1 58 04 61 00

**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 Australia, Pty., Ltd  
Level 17, 99 Walker Street  
North Sydney  
NSW 2059 Australia  
www.cisco.com  
Tel: +61 2 8448 7100  
Fax: +61 2 9957 4350

**Cisco Systems has more than 200 offices in the following countries and regions. Addresses, phone numbers, and fax numbers are listed on the Cisco.com Web site at [www.cisco.com/go/offices](http://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

All contents are Copyright © 1992–2001 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement. Printed in the USA. SMARTnet is a trademark; and Cisco, Cisco IOS, Cisco Systems, and Cisco Systems logo are registered trademarks of Cisco Systems, Inc. or its affiliates in the U.S. and certain other countries.

All other brands, names, or trademarks mentioned in this document or Web site are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0102R)