Mac OS X Server Fundamentals

UNIX power, open standards, and incredible ease of use.

Features

Open source UNIX-based foundation
- Kernel based on BSD and Mach 3.0
- Fine-grained multithreading
- Symmetric multiprocessing

Standards-based networking
- BSD networking with support for IPv4, IPv6, and IPSec
- Multilink multihoming
- Ethernet link aggregation with network interface failover

64-bit computing
- 64-bit memory addressing
- Optimized 64-bit math and image libraries

Security and access controls
- Common Data Security Architecture (CDSA)
- Access control lists (ACLs) and service ACLs
- IP firewall (IPFW2)

Directory services and authentication
- Open Directory architecture
- LDAPv3 and Active Directory integration
- RFC-compliant schema
- Single sign-on using Kerberos

File system
- Robust 64-bit HFS+ file system
- Long filenames and international support
- Case-sensitivity option
- File system journaling
- Software RAID levels 0, 1, and 10

High-availability services
- Watchdog
- IP failover
- Automatic restart
- Disk space monitoring

Mac OS X Server combines the latest open source technologies with Apple's industry-leading manageability and ease of use. The result is an industrial-strength server operating system that is easy and affordable to deploy and maintain.

The power of Mac OS X Server is a reflection of Apple's operating system strategy, one that favors open industry standards over proprietary technologies. It begins with an open source core and BSD networking architecture—delivering the capabilities you expect of a UNIX operating system, such as fine-grained multithreading, symmetric multi-processing, and protected memory. Mac OS X Server provides a stable, high-performance platform for deploying groundbreaking enterprise applications and services.

Apple extends the capabilities of Mac OS X Server by building on the best open source projects, such as Samba 3, NFS, OpenLDAP, MIT Kerberos, Postfix, and Apache. In fact, Mac OS X Server version 10.4 integrates more than 100 open source projects and enhances them with a unified management interface. This means you can deliver industry-standard network services virtually as soon as you open the box—without the complexities inherent in other UNIX-based solutions.

Built on open standards, Mac OS X Server is compatible with existing network and computing infrastructures. It uses native protocols to deliver directory services, file and printer sharing, and secure network access to Mac, Windows, and Linux clients. New support for access control lists (ACLs) provides flexible file system permissions that are compatible with Windows Server 2003 and Windows XP. A standards-based directory services architecture offers centralized management of network resources using any LDAP server—even proprietary servers such as Microsoft Active Directory. What's more, the open source UNIX-based foundation enables you to port existing tools to Mac OS X Server for fast and easy deployment.

While Mac OS X Server has the same robust core as Mac OS X, it adds industrial-strength features required for business-critical server deployments. Designed for "headless" operation, Mac OS X Server enables you to install and configure services without needing to connect a monitor to the server. Powerful remote management tools allow you to securely manage services from anywhere on the network or over the Internet, and support for SSH provides secure access from the UNIX command line. To keep your systems up and running, Mac OS X Server has built-in tools for monitoring systems, preventing accidental shutdown, and recovering services quickly in case of network or power failure.

UNIX Foundation: Darwin Kernel and BSD

Open source development model
Apple has released components of Mac OS X Server, including the UNIX-based core, to the open source development community. As a result of extensive peer reviews, Mac OS X Server v10.4 is a more robust and secure operating system.

The core of Mac OS X Server is known as Darwin, the same open source foundation used on Mac OS X, Apple's operating system for desktop and mobile computers. Darwin provides Mac OS X Server with the stability, performance, and reliability associated with UNIX.

At the heart of Darwin is the Mach 3.0 microkernel—based on the OSF/mk project from the Open Source Foundation. The Mach kernel provides services for memory management, thread control, hardware abstraction, and interprocess communication. In addition, Darwin includes the latest technological advances from the open source BSD community. Originally developed at the University of California, Berkeley, the BSD distribution is the foundation of most UNIX implementations today. Darwin is based largely on the FreeBSD distribution and includes the latest advances from this development community.

Building on this rich heritage, Apple delivers advanced server operations that include:

- **Fine-grained multithreading.** The kernel in Mac OS X Server provides superior thread management for efficient handling of multithreaded applications, whether the threads are running on one or multiple processors. It also provides precise control of real-time processing requirements, allowing a user-level thread, even an unprivileged one, to precisely specify its requirements for time-sensitive operations. Mac OS X Server implements POSIX threads (from POSIX 1003.1c standard), ensuring that each thread can be scheduled independently for maximum efficiency.

Kernel resource locking
Mac OS X Server v10.4 includes optimized kernel resource locking, which minimizes thread contention when using multiple processors. This allows users to get maximum performance from multiprocessor systems such as the Xserve G5 or Power Mac G5.

- **Symmetric multiprocessing (SMP).** Mac OS X Server harnesses all the available processing power in multiprocessor systems, enabling applications to benefit immediately from the exceptional performance of multiple processors. Complex tasks—such as numerical calculations, database queries, and compression and encoding operations—can take a long time to complete when they are done consecutively. With multiple processors working in parallel, multiple tasks can execute in little more than the time required to complete each task on a single processor. Because Mac OS X Server is multithreaded, services benefit from multiple processors even with applications that do not take advantage of the multiple threads.
- **Unified Buffer Cache.** To minimize disk access and the use of wired kernel memory, most UNIX systems enable the file system and virtual memory subsystems to share kernel buffers. Mac OS X Server utilizes this approach and automatically maps physical memory and on-disk files into virtual memory to minimize the use of system resources.
- **64-bit services.** Mac OS X Server features kernel and system software libraries updated specifically for the 64-bit PowerPC G5 processor. With full 64-bit memory addressing, applications can now break through the 4GB physical memory barrier, allowing them to deal with large data sets commonly found in scientific computing, databases, and multimedia solutions. The math and vector libraries have been tuned to take maximum advantage of new and faster math functions supported by the 64-bit PowerPC G5 processor.

Advanced Networking Architecture

Mac OS X Server is built on open, industry-standard protocols and the latest in network security standards to increase the performance and security of server deployments. Using the time-tested BSD sockets and TCP/IP stack, this advanced networking architecture ensures compatibility and integration with IP-based networks.

- **Multilink multihoming.** Multilink multihoming enables Mac OS X Server to host multiple IP addresses on the same or multiple network interfaces. This is ideal for connecting your server simultaneously to multiple networks, such as a public and a private network, or hosting multiple websites, each with its own IP address.
- **IPv6.** Most services in Mac OS X Server have been updated to support Internet Protocol version 6, or IPv6. The Internet Engineering Task Force (IETF) designed this next-generation protocol to replace the 20-year-old Internet Protocol version 4, or IPv4—still used in most of today's Internet sites. IPv6 fixes a number of problems in IPv4, such as the limited number of available addresses, and adds functionality in areas such as routing and network autoconfiguration. To support the industrywide IP transition, Mac OS X Server includes an IPv4-to-IPv6 gateway that enables the deployment of IPv4-based server services in IPv6 networks.
- **IPSec.** IPSec is a set of general-purpose protocols for protecting TCP/IP communications. Its network-layer cryptography mechanism provides privacy using data and packet-header encryption, integrity and packet-origin authentication, and key management. Although part of the IPv6 standard, IPSec can also be used with IPv4.
- **IP over FireWire.** Ideal for ad hoc network deployments and system administration, IP over FireWire allows you to create an inexpensive point-to-point IP network between two devices. IP over FireWire is also useful as a low-latency, high-bandwidth network in high-performance computing, application clustering, and IP failover scenarios.

Dual onboard Gigabit Ethernet
Xserve G5 features an advanced Ethernet controller on the main logic board, providing two independent Gigabit Ethernet interfaces and hardware support for VLAN, jumbo frames, and TCP and UDP hardware checksum.

- **Ethernet link aggregation with network interface failover.** Also known as IEEE 802.3ad, link aggregation allows you to configure multiple network interfaces to appear as a single interface—with the same MAC address, the same IP address, and the same server host name. This provides two significant benefits. It multiplies the potential I/O performance by the number of interfaces; for example, two 1-gigabit interfaces bonded together can provide up to 2 gigabits of aggregate network bandwidth, and four 1-gigabit interfaces can provide up to 4 gigabits. Link aggregation also eliminates a potential single point of failure: If one interface fails, the remaining interface maintains the network connection. Ethernet link aggregation is supported by Xserve G5 systems and by systems with third-party Ethernet cards that conform to the IEEE 802.3ad standard.
- **VLAN.** Mac OS X Server on Xserve G5 systems supports virtual local area networks (VLANs). This feature allows you to configure computers on different network sections to behave as though they were on the same section. For example, with a VLAN, people in a workgroup who are located on different floors or in different buildings can appear as though they are on the same local network.
- **Jumbo frames.** Mac OS X Server supports jumbo frames, or packets larger than 1518 bytes. By packing more data in fewer packets, jumbo frames can increase network efficiency and throughput, while reducing demands on the processor. Jumbo frames require compatible hardware and clients that can accept jumbo frames.
- **802.1X network authentication.** 802.1X authentication minimizes security risks on wired Ethernet networks by providing computer identification, centralized authentication, and encryption. 802.1X supports the Extensible Authentication Protocol (EAP), which enables you to use different authentication methods such as tokens, smart cards, and SSL certificates.

64-Bit Computing

One operating system
Apple's strategy is to deliver a single operating system for all Apple computers, whether they're 32-bit processor–based consumer systems or 64-bit processor–based desktop computers and rackmount servers. This "one system" approach ensures software and device compatibility across the broadest-possible range of Apple hardware.

Apple has written Mac OS X Server v10.4 to leverage the 64-bit features of the PowerPC G5 architecture, bringing next-generation power to mainstream server computing. With superaccurate math calculations and access to massive amounts of memory, Mac OS X Server is the ideal platform for the most demanding scientific and technical computing needs.

While Mac OS X Server and the PowerPC G5 are the perfect platform for next-generation networking applications and services, they also run today's 32-bit applications natively. In fact, unmodified 32-bit application code takes immediate advantage of faster processor clock speeds. Performance gains are even more dramatic when applications are recompiled for the PowerPC G5. Developers can use Apple's Xcode tools to optimize their software for maximum performance on PowerPC G5–based systems.

64-bit applications
With Mac OS X Server v10.4, Apple delivers 64-bit memory addressing without compromising performance and support for 32-bit applications. 64-bit memory addressing makes it possible to run applications with data sets that require more than 4GB of memory, ideal for high-performance server applications, computational engines, and other command-line applications. Loading large data sets into memory improves application performance and data access times significantly, because memory access is up to 40 times faster than disk access. In addition, some analytical applications that require the manipulation of large data sets in contiguous memory, such as genome assembly, can be performed only on systems with 64-bit memory addressing.

Mac OS X Server supports the standard LP64 data model, which means that code written for other 64-bit UNIX-based systems can easily be ported to Mac OS X Server.

Apple's SAN file system
Mac OS X Server can be used with Xsan, Apple's 64-bit cluster file system for storage area networks. With Mac OS X Server v10.4, Xsan can access and host individual volumes of up to 2 petabytes.

64-bit file system
Mac OS X Server features a high-performance 64-bit file system that supports HFS+ (and HFS+ journaled) file systems beyond the 16TB limit of a 32-bit file system. This enables you to create very large, exabyte-size volumes for massive databases, image archives, and digital video storage.

64-bit math and image libraries
Mac OS X Server includes optimized libraries that take advantage of the faster math functions supported by the 64-bit PowerPC G5. These advanced routines use the best-possible functionality for a specific PowerPC processor, with optimum performance on the PowerPC G5. Existing 32-bit applications that use the new math libraries will benefit—without modification—from these enhancements. Updated math, vector, and image processing routines include:

- Double-precision transcendental functions (libm)
- Vectorized transcendental functions (vMathLib)
- 128-bit integer math (vBigNum)
- Basic Linear Algebra Subprograms (BLAS)
- Linear Algebra Package (LAPACK)
- Vectorized digital signal processing (vDSP)
- Vector image processing (vImage)

Security and Access Controls

Security and open source
Apple's open source development approach makes Mac OS X Server a more secure operating system—its core components have been subjected to years of public scrutiny from developers and security experts around the world. Because anyone can freely inspect the source code, identify theoretical vulnerabilities, and take steps to strengthen the software, open source software benefits from strong security.

Mac OS X Server is built on a robust UNIX foundation that contains many security features in its core architecture. State-of-the-art, standards-based technologies protect your server, your network, and your organization's data, including built-in firewall with stateful packet analysis, strong encryption and authentication services, data security architectures, and support for access control lists (ACLs). Simple interfaces and configuration tools allow you to configure systems easily and securely. In fact, when you take an Apple server out of the box, it's already securely configured.

For more information about security features built into Mac OS X and Mac OS X Server, see www.apple.com/macosx/features/security.

Security standards

Trusted by security experts around the world, industry-standard security protocols support all aspects of system, data, and networking security required by today's applications.

Rapid response
Because the security of your systems is so important, Apple responds rapidly to provide patches and updates. Apple works with worldwide partners, including the Computer Emergency Response Team (CERT), to notify you of potential threats. Should vulnerabilities be discovered, the built-in Software Update tool sends notification of security updates, which are made available for easy download and installation.

- **Kerberos for single sign-on.** Mac OS X Server integrates MIT's Kerberos technology to enable single sign-on in both Apple Open Directory and Microsoft Active Directory environments.
- **SSH (Secure Shell).** Mac OS X Server uses OpenSSH as its default protocol for secure remote server setup and administration. SSH encrypts remote command-line traffic, including passwords, to effectively eliminate eavesdropping, connection hijacking, and other network-level attacks that plague rlogin and telnet connections. Mac OS X Server includes the full suite of OpenSSH client and server functionality, including SSH for command execution, SFTP for file transfer, and SCP for file copies.
- **SSL/TLS.** Mac OS X Server integrates Secure Sockets Layer (SSL), today's most common transport mechanism, and Transport Layer Security (TLS), the next-generation security standard for the Internet. The core server operating system and many network services, including Apache, OpenLDAP, Postfix, and Cyrus, use these transport layer mechanisms to provide a secure, 128-bit encrypted channel between two systems and to protect the information in the channel from eavesdroppers. For secure authenticated communications, Mac OS X Server can use X.509 digital certificates to verify a server's authenticity on the Internet or local area network.
- **CDSA (Common Data Security Architecture).** Mac OS X Server uses CDSA, an open standard from the Open Group. CDSA provides a layered set of security services and a cryptographic framework for creating security-enabled applications, including support for SSL versions 2 and 3 and TLS version 1. Apple's CDSA architecture also integrates OpenSSL, a security library for use by legacy open source applications, as well as the Linux Pluggable Authentication Modules (PAMs), allowing UNIX applications to access CDSA services through a PAM API.

File system ACLs
Apple's ACL implementation is compatible with POSIX 1003e draft. This enables full interoperability with the native permissions of Windows Server 2003 and Windows XP, while maintaining backward compatibility with traditional UNIX file permissions.

Access control lists (ACLs)

Mac OS X Server v10.4 is the only UNIX-based server operating system that supports the native rich file permissions of Mac OS X and Windows. Access control lists (ACLs) give administrators fine-grained control over server settings and permissions, protecting applications and data from unauthorized use and modification.

File system access. Mac OS X Server v10.4 supports both traditional UNIX file permissions and ACLs, offering administrators an unprecedented level of control over file and folder permissions. Most UNIX- and Linux-based operating systems are constrained by the UNIX file permissions model, also known as Standard Portable Operating System Interface (POSIX) permissions. Standard UNIX file permissions allow you to assign one access privilege to the file's owner, one to a group, and one to everyone on the

Common Criteria certification
The Common Criteria is an internationally approved set of security standards, designed to provide a clear and reliable evaluation of the security capabilities of technology products. For more information, download Apple's Common Criteria Certification white paper at www.apple.com/federal/security.

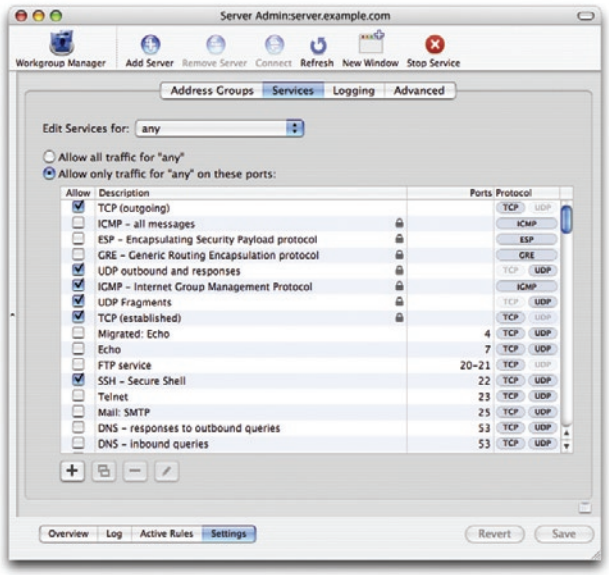
network. Multiple users and multiple groups are not allowed, nor is ownership by a group. The traditional UNIX model also lacks other important file access features: It supports only three permissions—read, write, and execute—and does not support permission inheritance, which enables new or copied files to automatically inherit the access controls of the parent directory.

To provide greater flexibility in complex computing environments, Apple has added support for ACLs in Mac OS X Server v10.4. With file system ACLs, any file object can be assigned multiple users and groups, including groups within groups. Each file object can also be assigned both allow and deny permissions, as well as a granular set of permissions for administrative control, read, write, and delete operations. For added security, Mac OS X Server supports a file permission inheritance model, ensuring that user permissions are inherited when files are moved to the server and rewritten when files are copied to the server.

Service access. Service access control lists (SACLs) provide a simple way for server administrators to specify which users and groups can access different services. For example, an administrator can configure a workgroup file server bound to a huge centralized directory to accept connections only from users who are in the workgroup. This capability is increasingly critical, as more sites are moving to a centralized directory system. All the user-based Mac OS X Server services—including AFP, SMB/CIFS, FTP, Web, Mail, SSH, iChat Server, and VPN—support SACLs.

Firewall

Similar to erecting a wall that restricts access, firewall software protects network applications running on Mac OS X Server. Using the reliable, open source IPFW software from FreeBSD, the firewall in Mac OS X Server scans incoming IP packets and rejects or accepts them based on the filters you set. You can restrict access to any IP service running on the server, and you can customize filters for all incoming clients or for a range of client IP addresses. To prevent IP address spoofing, the firewall software provides stateful packet inspection, which determines whether an incoming packet is a legitimate response to an outgoing request or part of an ongoing session.



The Server Admin application in Mac OS X Server allows you to configure firewall rules and settings with simple on/off checkboxes and human-readable names.

Directory Services and Authentication

A key component of any modern computing environment, directory services allow organizations to centralize information about users, groups, and computing resources. This network-based repository is the foundation for critical IT services, including managing users and groups, directing workflow solutions, providing employee directories, and controlling access privileges. By maintaining a central directory, organizations can consolidate resources, simplify system management, and reduce support and administration costs—while providing strong authentication and password-protected access to network resources.

Mac OS X Server features Open Directory, Apple's directory and authentication services architecture. Based on the LDAPv3 standard, the Open Directory architecture allows you to integrate your server with any LDAP directory, leveraging the directory services in existing network infrastructures.

Integration with directory services
Based on open standards, Apple's Open Directory architecture features built-in directory access modules that simplify integration with third-party services, including Microsoft Active Directory, Novell eDirectory, OpenLDAP, SunONE, NIS, and NetInfo.

Directory services

To simplify the deployment of Mac OS X systems in existing infrastructures, Apple has adhered to published open standards, including OpenLDAP and the RFC 2307 schema. The Open Directory architecture comes with directory access modules for various popular directory services solutions. It also allows for customized schema mappings, so attributes in an LDAP-based directory can be mapped to settings on the Mac—eliminating the need to configure each client system. Apple has published these extensions as part of a comprehensive open source project that includes all interoperability components.

Single sign-on

Mac OS X Server integrates an authentication authority based on MIT's Kerberos technology, supporting single sign-on in both Apple Open Directory and Microsoft Active Directory environments. Kerberos uses encryption keys to provide strong authentication for client/server applications, allowing authorized users to access secure network services—without exchanging passwords or requiring users to type in their passwords repeatedly.

Using strong Kerberos authentication, single sign-on maximizes security while providing users with easier access to a broad range of Kerberos-enabled network services, including Login, SSH, AFP, SMB/CIFS, FTP, SMTP, IMAP, POP, Xgrid, WebDAV, Web, and VPN services. Even in mixed-platform environments, users can enter the same user name and password to access their home directories, group file servers, or other resources from any system on the network—Mac, Windows, or Linux. Not only does single sign-on simplify the user experience, but it can dramatically reduce the time that support technicians spend resetting forgotten passwords.

Open Directory Server also uses Simple Authentication and Security Layer (SASL) to support legacy authentication protocols, including NT and LAN Manager, CRAM-MD5, APOP, Diffie-Hellman Exchange, and Two-Way Random. For any service that isn't Kerberos enabled, SASL automatically negotiates the strongest supported authentication method. Using Server Admin, you can enable or disable individual protocols. Since authentication is conducted on the user level, you can mix and match authentication methods for different types of users connecting to your server.

File System

Support for local file systems
Loadable file systems based on BSD's stackable virtual file system (vfs) layer allow Mac OS X Server to dynamically mount, read, and write to numerous local file systems—including HFS+, UFS, ISO 9660 CD-ROM formats, UDF for DVDs, FAT32, and NTFS (read only)—enabling your media to work on Mac OS X Server without modification.

Mac OS X Server supports the Mac OS Extended file system and UNIX File System (UFS). Apple's Mac OS Extended file system is a robust HFS+ file system designed and optimized for critical server deployments. It supports 64-bit disk space addressing and features 32-bit file allocation blocks—maximizing disk efficiency by decreasing the disk space usage on large volumes and volumes containing a large number of files. In addition, support for the Berkeley FFS–based UFS and standard POSIX semantics enables Mac OS X Server to access and host data from traditional UNIX file systems.

The Mac OS Extended file system includes these powerful features:

- **Long filenames and international support.** Mac OS X Server allows more descriptive filenames, with support for up to 255 characters and Unicode text encoding for international and mixed-script filenames.
- **Case sensitivity.** Mac OS X Server offers an optional case-sensitive file system format for HFS+, allowing administrators to safely host files for use by UNIX applications that require case sensitivity.
- **File system journaling.** A robust journaling feature protects the integrity of the file system in the event of an unplanned shutdown or power failure. With journaling in Mac OS X Server, the server automatically tracks file system operations and maintains a continuous record of these transactions in a separate file, called a journal. After an unexpected shutdown, the operating system can use the journal to return the file system to a known state—eliminating the need to perform a consistency check on the entire file system during startup. With a journaled file system, bringing a volume back online takes just seconds, regardless of the number of files or the size of the volume.
- **Software RAID.** Mac OS X Server supports drive striping (RAID 0) for improved performance, drive mirroring (RAID 1) for improved reliability, and mirrored striping (RAID 10) for improving both performance and reliability of server storage. In addition, Mac OS X Server v10.4 allows you to reformat storage in the background: You can promote a single volume to a mirrored volume, split a mirrored array into two volumes (demotion), or rebuild RAID volumes—without server downtime.

High-Availability Services

Real-time information about Xserve systems
Server Monitor allows administrators to review information about hundreds of Xserve systems from any Internet-connected Mac OS X system.

To guarantee service levels, comply with industry regulations, or provide access to business-critical information, organizations demand the highest-possible availability of computing services. Events that may once have been considered minor, such as unplanned shutdowns, can now severely impair operations. Apple has built into Mac OS X Server powerful high-availability features that reduce the risk of shutdowns and maximize server uptime.

- **Watchdog.** For maximum availability, Mac OS X Server includes a watchdog process that continuously monitors activity and recovers services in the event of an application, system, or power failure.
- **IP failover.** When Mac OS X Server is used with two servers, the IP failover service further increases availability. If one server fails, the second server can take over the IP address and deliver services for the failed server.
- **Automatic restart.** Mac OS X Server can be set to restart automatically in case of a power failure or catastrophic system failure.
- **Disk mirroring.** RAID 1, or disk mirroring, is a common technique for eliminating single points of failure. Copies of the same data are mirrored on two or more drives—reducing the risk of service shutdown if one of the disks were to fail.

- **Disk space monitoring.** Running out of disk space can reduce the reliability of your server. Mac OS X Server includes tools that monitor disk space and proactively free up space by deleting or backing up noncritical logs and utilities.

Apple Server and Storage Solutions

Combining the latest open source technologies with Apple's industry-leading manageability and ease of use, Mac OS X Server unleashes the power of Xserve G5, Apple's rack-optimized server hardware. With phenomenal performance, massive storage capacity, high-bandwidth I/O, and built-in remote management tools, Xserve G5 running Mac OS X Server is an unparalleled server solution for businesses, schools, and research centers. For even more capacity, organizations can add Xserve RAID storage systems—and share terabytes of data over an ultrafast Fibre Channel network with Xsan, Apple's SAN file system. With unmatched integration between hardware and software, Apple's server and storage products allow you to extend your computing infrastructure while lowering your management and maintenance costs.

For More Information

For more information about Mac OS X Server, Xsan, Xserve, and other Apple server solutions, visit www.apple.com/macosx/server.