



OS X Mountain Lion

Core Technologies Overview
June 2012



Contents

Page 3	Introduction
Page 4	System Startup BootROM EFI Kernel Drivers Initialization Address Space Layout Randomization (ASLR)
Page 7	Disk Layout Partition scheme Core Storage File systems
Page 9	Process Control Launchd Loginwindow Grand Central Dispatch Sandboxing GateKeeper XPC
Page 16	Network Access Ethernet Wi-Fi Multihoming IPv6 Remote Access Bonjour
Page 21	Document Lifecycle Auto Save Automatic Versions Version Management iCloud Storage
Page 24	Data Management Spotlight Time Machine
Page 26	Developer Tools LLVM Xcode Instruments Accelerate Automation WebKit
Page 33	For More Information

Introduction



With more than 65 million users—consumers, scientists, animators, developers, system administrators, and more—OS X is the most widely used UNIX® desktop operating system. In addition, OS X is the only UNIX environment that natively runs Microsoft Office, Adobe Photoshop, and thousands of other consumer applications—all side by side with traditional command-line UNIX applications. Tight integration with hardware—from the sleek MacBook Air to the powerful Mac Pro—makes OS X the platform of choice for an emerging generation of power users.

This document explores the powerful industry standards and breakthrough innovations in the core technologies that power Apple's industry-leading user experiences. We walk you through the entire software stack, from firmware and kernel to iCloud and developer tools, to help you understand the many things OS X does for you every time you use your Mac.

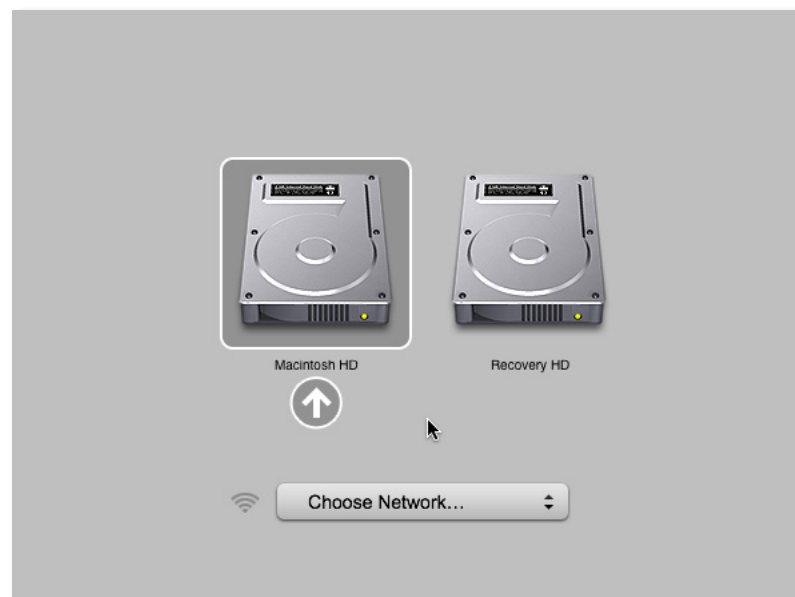
System Startup

BootROM

When you turn on the power to a Mac, it activates the BootROM firmware. BootROM, which is part of the computer's hardware, has two primary responsibilities: it initializes system hardware and it selects an operating system to run. Two BootROM components carry out these functions:

- Power-On Self Test (POST) initializes some hardware interfaces and verifies that sufficient memory is available and in a good state.
- Extensible Firmware Interface (EFI) does basic hardware initialization and selects which operating system to use.

If multiple OS installations are available, BootROM chooses the one that was last selected by the Startup Disk System Preference. The user can override this choice by holding down the Option key while the computer starts up, which causes EFI to display a screen for choosing the startup volume.



EFI boot picker screen.

EFI

EFI—a standard created by Intel—defines the interface between an operating system and platform firmware. It supersedes the legacy Basic Input Output System (BIOS) and OpenFirmware architectures.

Once BootROM is finished and an OS X partition has been selected, control passes to the boot.efi boot loader, which runs inside EFI. The principal job of this boot loader is to load the kernel environment. As it does this, the boot loader draws the “booting” image on the screen.

If full-disk encryption is enabled, the boot loader draws the login UI and prompts for the user’s password, which the system needs so it can access the encrypted disk and boot from it. Otherwise, loginwindow draws the login UI.

Kernel

The OS X kernel is based on FreeBSD and Mach 3.0 and features an extensible architecture based on well-defined kernel programming interfaces (KPIs).

OS X was the first operating system to ship as a single install that could boot into either a 32-bit or 64-bit kernel, either of which could run 32-bit and 64-bit applications at full native performance. Starting with Mountain Lion, OS X exclusively uses a 64-bit kernel, but it continues to run both 32-bit and 64-bit applications.

Drivers

Drivers in OS X are provided by I/O Kit, a collection of system frameworks, libraries, tools, and other resources for creating device drivers. I/O Kit is based on an object-oriented programming model implemented in a restricted form of C++ that omits features unsuitable for use within a multithreaded kernel.

By modeling the hardware connected to an OS X system and abstracting common functionality for devices in particular categories, the I/O Kit streamlines the process of device-driver development. I/O Kit helps device manufacturers rapidly create drivers that run safely in a multiprocessing, preemptive, hot-pluggable, power-managed environment.

To do this, I/O Kit provides the following:

- An object-oriented framework implementing common behavior shared among all drivers and types (families) of drivers
- Many families of drivers for developers to build upon
- Threading, communication, and data-management primitives for dealing with issues related to multiprocessing, task control, and I/O-transfers
- A robust, efficient match-and-load mechanism that scales well to all bus types
- The I/O Registry, a database that tracks instantiated objects (such as driver instances) and provides information about them
- The I/O Catalog, a database of all I/O Kit classes available on a system
- A set of device interfaces—plug-in mechanism that allows applications and other software outside the kernel to communicate with drivers
- Excellent overall performance
- Support for arbitrarily complex layering of client and provider objects

Initialization

There are two phases to system initialization:

- *boot* refers to loading the bootstrap loader and kernel
- *root* means mounting a partition as the root, or top-level, file system.

Once the kernel and all drivers necessary for booting are loaded, the boot loader starts the kernel's initialization procedure. At this point, enough drivers are loaded for the kernel to find the root device—the disk or network service where the rest of the operating system resides.

The kernel initializes the Mach and BSD data structures and then initializes the I/O Kit. The I/O Kit links the loaded drivers into the kernel, using the device tree to determine which drivers to link. Once the kernel finds the root device, it roots BSD off of it.

Address Space Layout Randomization (ASLR)

Many malware exploits rely on fixed locations for well-known system functions. To mitigate that risk, Mountain Lion randomly relocates the kernel, kexts, and system frameworks at system boot. This protection is available to both 32-bit and 64-bit processes.

Disk Layout

Partition scheme

Disk drives are divided into logical partitions, which Apple traditionally calls *volumes*. Modern Mac systems use the GUID partition table (GPT) partitioning scheme introduced by Intel as part of EFI. The partitioning scheme is formally defined by:

- Section 11.2.2 of “Extensible Firmware Interface Specification,” version 1.1, available from [Intel](#)
- Chapter 5, “GUID Partition Table (GPT) Format,” of the “Unified Extensible Firmware Interface Specification,” version 2.0, available from the [Unified EFI Forum](#)

Any Mac running OS X 10.4 or later can mount GPT-partitioned disks. Intel-based Mac systems can boot from GPT. By default, the internal hard disk is formatted as GPT.

You can explore and modify GPT disks using the `gpt` command-line tool derived from FreeBSD. You can also use Apple’s GPT-aware `diskutil` utility which provides more human-readable output.

Helper partitions

Typically a single partition is “blessed” as the active boot volume via the `bless` command-line tool, though you can also bless specific folders or files. This partition is usually also the root volume.

However, sometimes the boot partition is not the root, such as when the root partition is encrypted using full-disk encryption or located on a device that requires additional drivers (such as a RAID array). In that case, a hidden helper partition stores the files needed to boot, such as the kernel cache. The last three known good helper partitions are maintained in case one becomes corrupted.

Recovery partitions

OS X Lion introduced a new Recovery HD partition that includes the tools you need to do the following:

- Reinstall OS X
- Repair a hard drive
- Restore from a Time Machine backup
- Launch Safari to view documentation and search the Internet
- Create Recovery HD partitions on external drives.

To boot from the Recovery HD partition, restart your Mac while holding down the Command key and the R key (Command-R). Keep holding them until the Apple icon appears, indicating that your Mac is starting up. After the Recovery HD finishes starting up, you should see a desktop with an OS X menu bar and an OS X Utilities application window.

If your Recovery HD is corrupt or unavailable and you have a network connection, your Mac will automatically use OS X Internet Recovery to download and boot directly from Apple's servers, using a pristine Recovery HD image that provides all the same functionality.

Core Storage

Layered between the whole-disk partition scheme and the file system used for a specific partition is a new logical volume format known as Core Storage, introduced in OS X Lion. Core Storage makes it easy to dynamically allocate partitions while providing full compatibility with existing filesystems. In particular, Core Storage allows in-place transformations such as backgrounding the full-disk encryption used by File Vault 2.

File systems

Partitions are typically formatted using some variant of the HFS Plus file system, which provides fast Btree-based lookups, robust aliases, and rich metadata—including fine-grained access controls and extended attributes. Since OS X 10.3 Panther, every Mac has used a journaled version of HFS Plus (HFSJ) to improve data reliability. Since OS X 10.6 Snow Leopard, HFS Plus has automatically compressed files.

You can also choose to format partitions with HFSX, a case-sensitive variant of HFS Plus intended for compatibility with UNIX software. For interoperability with Windows, systems disks may be formatted with FAT32 or exFAT.

Process Control

Launchd

The kernel invokes `launchd` as the first process to run and then bootstraps the rest of the system. It replaces the complex web of `init`, `cron`, `xinetd`, and `/etc/rc` used to launch and manage processes on traditional UNIX systems. `launchd` first appeared in OS X 10.4 Tiger. It is available as open source under the Apache license.

File-based configuration

Each job managed by `launchd` has its own configuration file in a standard `launchd.plist(5)` file format, which specifies the working directory, environment variables, timeout, Bonjour registration, etc. These plists can be installed independently in the standard OS X library domains (for example, `/Network/Library`, `/System/Library`, `/Library`, or `~/Library`), avoiding the need to edit system-wide configuration scripts. Jobs and plists can also be manually managed by the `launchctl(1)` command-line tool.

Launch on demand

`launchd` prefers for processes to run only when needed instead of blocking or polling continuously in the background. These launch-on-demand semantics avoid wasting CPU and memory resources, and thus prolong battery life.

For example, jobs can be started based on the following:

- If the network goes up or down
- When a file path exists (e.g., for a printer queue)
- When a device or file system is mounted

Smart scheduling

Like traditional UNIX cron jobs, `launchd` jobs can be scheduled for specific calendar dates with the `StartCalendarInterval` key, as well as at generic intervals via the `StartInterval` key. Unlike `cron`—which skips job invocations when the computer is asleep—`launchd` starts the job the next time the computer wakes up. If the computer sleeps through multiple intervals, those events will be coalesced into a single trigger.

User agents

`launchd` defines a daemon as a system-wide service where one instance serves multiple clients. Conversely, an agent runs once for each user. Daemons should not attempt to display UI or interact directly with a user's login session; any and all work that involves interacting with a user should be done through agents.

Every `launchd` agent is associated with a Session Type, which determines where it runs and what it can do, as shown in the following table:

Name	Session type	Notes
GUI	Aqua	Has access to all GUI services; much like a login item
Non-GUI	StandardIO	Runs only in non-GUI login sessions (for example, SSH login sessions)
Per-user	Background	Runs in a context that's the parent of all contexts for a given user
Pre-login	LoginWindow	Runs in the loginwindow context

Install on demand

To reduce download sizes and the surface area available to attackers, OS X provides an install-on-demand mechanism for certain subsystems. This provides easy access for those users who need them without burdening those who don't. When you launch an application that relies on X11 or Java, OS X asks whether you want to download the latest version as shown in the next image.



OS X prompts users if they attempt to run applications that require X11.

Loginwindow

As the final part of system initialization, `launchd` launches `loginwindow`. The `loginwindow` program controls several aspects of user sessions and coordinates the display of the login window and the authentication of users.

If a password is set, OS X requires users to authenticate before they can access the system. The `loginwindow` program manages both the *visual* portion of the login process (as manifested by the window where users enter name and password information) and the *security* portion (which handles user authentication).

Once a user has been authenticated, `loginwindow` begins setting up the user environment. As part of this process, it performs the following tasks:

- Secures the login session from unauthorized remote access
- Records the login in the system's `utmp` and `utmpx` databases
- Sets the owner and permissions for the console terminal
- Resets the user's preferences to include global system defaults
- Configures the mouse, keyboard, and system sound according to user preferences
- Sets the user's group permissions (`gid`)

- Retrieves the user record from Directory Services and applies that information to the session
- Loads the user's computing environment (including preferences, environment variables, device and file permissions, keychain access, and so on)
- Launches the Dock, Finder, and SystemUIServer
- Launches the login items for the user

Once the user session is up and running, `loginwindow` monitors the session and user applications in the following ways:

- Manages the logout, restart, and shutdown procedures
- Manages Force Quit by monitoring the currently active applications and responding to user requests to force quit applications and relaunch the Finder. (Users open this window from the Apple menu or by pressing Command-Option-Escape.)
- Arranges for any output written to the standard error console to be logged using the Apple System Logger (ASL) API. (See ["Log Messages Using the ASL API"](#) in the OS X Developer Library.)

Grand Central Dispatch

Grand Central Dispatch (GCD) supports concurrent computing via an easy-to-use programming model built on highly efficient system services. This radically simplifies the code needed for parallel and asynchronous processing across multiple cores.

GCD is built around three core pieces of functionality:

- Blocks, a concise syntax for *describing* work to be done
- Queues, an efficient mechanism for *collecting* work to be done
- Thread pools, an optimal service for *distributing* work to be done

These help your Mac make better use of all available CPU cores while improving responsiveness by preventing the main thread from blocking.

System-wide optimization

The central insight of GCD is shifting the responsibility for managing threads and their execution from applications to the operating system. As a result, programmers can write less code to deal with concurrent operations in their applications, and the system can perform more efficiently on both single-processor and multiprocessor machines. Without a pervasive approach such as GCD, even the best-written application cannot deliver optimal performance across diverse environments because it lacks insight into everything else happening on the system.

Blocks

Block objects are extensions to C, Objective-C, and C++ that make it easy for programmers to encapsulate inline code and data for later use. Here's what a block object looks like:

```
int scale = 4;
int (^Multiply)(int) = ^(int num) {
    return scale * num;
};
int result = Multiply(7); // result is 28
```

These types of “closures”—effectively a function pointer plus its invocation context—are common in dynamically-typed interpreted languages, but they were never before widely available to C programmers. Apple has published both the Blocks Language Specification and its implementation as open source under the MIT license and added blocks support to both GCC and Clang/LLVM.

Queues

GCD dispatch queues are a powerful tool for performing tasks safely and efficiently on multiple CPUs. Dispatch queues atomically add blocks of code that can execute either asynchronously or synchronously. Serial queues enable mutually exclusive access to shared data or other resources without the overhead or fragility of locks. Concurrent queues can execute tasks across multiple distinct threads, based on the number of currently available CPUs.

Thread pools

The root level of GCD is a set of global concurrent queues for every UNIX process, each of which is associated with a pool of threads. GCD dequeues blocks and private queues from the global queues on a first-in/first-out (FIFO) basis as long as there are available threads in the thread pool, providing an easy way to achieve concurrency.

If there is more work than available threads, GCD asks the kernel for more threads, which are given if there are idle logical processors. Conversely, GCD eventually retires threads from the pool if they are unused or the system is under excessive load. This all happens as a side effect of queuing and completing work so that GCD itself doesn't require a separate thread. This approach provides optimal thread allocation and CPU utilization across a wide range of loads.

Event sources

In addition to scheduling blocks directly, GCD makes it easy to run a block in response to various system events, such as a timer, signal, I/O, or process state change. When the source fires, GCD will schedule the handler block on the specific queue if it is not currently running, or—more importantly—coalesce pending events if it is running. This provides excellent responsiveness without the expense of either polling or binding a thread to the event source. Plus, since the handler is never run more than once at a time, the block doesn't even need to be reentrant; only one thread will attempt to read or write any local variables.

OpenCL integration

Developers traditionally needed to write custom vector code—in addition to their usual scalar code—in order to take full advantage of modern processors. OpenCL is an open standard, language, runtime, and framework introduced in OS X 10.6 Snow Leopard. The OpenCL standard makes it straightforward take advantage of the immense processing power available in GPUs, vector extensions, and multi-core CPUs.

You can use OpenCL to move the most time-consuming routines into computational “kernels” written in a simple, C-like language. The OpenCL runtime dynamically compiles these kernels to take advantage of the type and number of processors available on a computer. As of OS X 10.7 Lion, the system takes care of autovectorizing kernels to run efficiently on GPUs or CPUs. OpenCL kernels can also be written as separate files that run as blocks on the GPU or CPU using a special GCD queue.

Sandboxing

Sandboxes ensure that processes are only allowed to perform a specific set of expected operations. For example, a web browser regularly needs to read from the network, but shouldn't write to the user's home folder without explicit permission. Conversely, a disk usage monitor may be allowed to read directories and delete files, but not talk to the network.

These restrictions limit the damage a program could potentially cause if it became exploited by an attacker. By using attack *mitigation*, sandboxes complement the usual security focus on attack *prevention*. For this reason, we recommend that sandboxes be used with all applications, and we require their use for apps distributed via the Mac App Store.

Mandatory access controls

Sandboxes are built on low-level access control mechanisms enforced in the kernel by the `kauth` subsystem. This was introduced in OS X 10.4 Tiger based on work originating in TrustedBSD. `kauth` identifies a valid actor (typically a process) by its credentials. It then asks one or more listeners to indicate whether that actor can perform a given action within a specified scope (authorization domain). Only the initial (default) listener can allow a request; subsequent listeners can only deny or defer. If all listeners defer, `kauth` denies the request.

Entitlements

Sandboxes collect these low-level actions into specific entitlements that an application must explicitly request by adding the appropriate key to a property list file in its application bundle. Entitlements can control access to:

- The entire file system
- Specific folders
- Networking
- iCloud
- Hardware (for example, the built-in camera or microphone)
- Personal information (for example, contacts)

In addition, entitlements control whether processes inherit their parents' permissions and can grant temporary exceptions for sending and receiving events or reading and writing files.

User intent

While it may seem that virtually all applications would need to request broad entitlements to read and write files, that isn't the case. OS X tracks user-initiated actions, such as dragging a file onto an application icon, and automatically opens a temporary hole in the sandbox allowing the application to read just that one file. In particular, open and save panels run in a special-purpose PowerBox process that handles all user interaction. This allows applications to only request entitlements for actions they need to perform autonomously.

Code signing

Entitlements use code signing to ensure the privileges they specify only cover the code originally intended. Code signing uses public key cryptography to verify that the entity that created the entitlements (that is, the developer) is the same as the author of the executable in question, and that neither has been modified.

GateKeeper

Gatekeeper is a new feature in OS X Mountain Lion that helps protect you from downloading and installing malicious software. Developers can sign their applications, plug-ins, and installer packages with a Developer ID certificate to let Gatekeeper verify that they come from identified developers.

Developer ID certificates

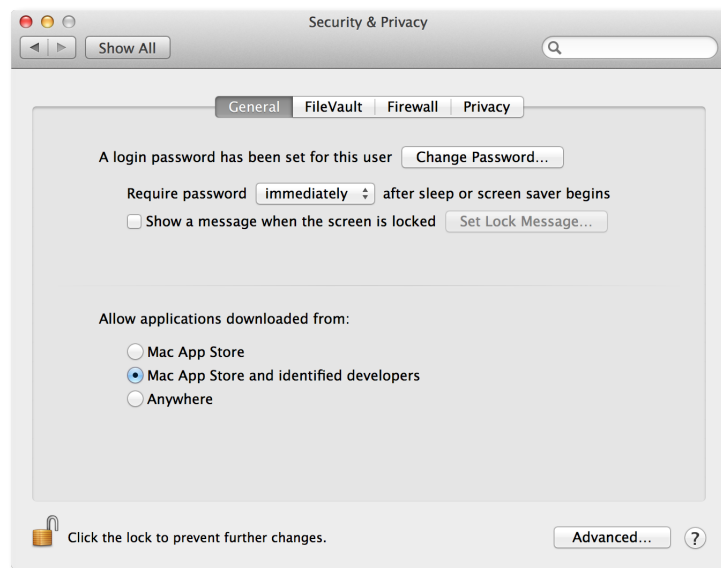
As part of the Mac Developer Program, Apple gives each developer a unique Developer ID for signing their apps. A developer's digital signature lets Gatekeeper verify that they have not distributed malware and that the app hasn't been tampered with.

User control

Choose the kinds of apps that are allowed to run on OS X Mountain Lion from the following:

- Only apps from the Mac App Store, for maximum security
- Apps from the Mac App Store as well as apps that have a Developer ID
- Apps from anywhere

You can even temporarily override higher-protection settings by clicking on the app while holding down the Control key and then choosing Open from the contextual menu. This lets you install and run any app at any time. Gatekeeper ensures that you stay completely in control of your system.



You control which kinds of apps you want your system to trust.

XPC

XPC leverages `launchd`, GCD, and sandboxing to provide a lightweight mechanism for factoring an application into a family of coordinating processes. This factoring improves launch times, crash resistance, and security by allowing each process to focus on one specific task.

No configuration needed

XPC executables and `xpcservice.plist` (5) configuration files are all part of a single app bundle, so there is no need for an installer.

Launch-on-demand

XPC uses `launchd` to register and launch helper processes as they are needed.

Asynchronous communication

XPC uses GCD to send and receive messages asynchronously using blocks.

Privilege separation

XPC processes each have their own sandbox, allowing clean separation of responsibilities. For example, an application that organizes and edits photographs does not usually need network access. However, it can create an XPC helper with different entitlements whose sole purpose is to upload photos to a photo sharing website.

Out of band data

In addition to primitive data types such as booleans, strings, arrays, and dictionaries, XPC can send messages containing out-of-band data such as file descriptors and `IOSurface` media objects.

Network Access

Ethernet

Mac systems were the first mass-market computers to ship with built-in Ethernet. OS X today supports everything from 10BASE-T to 10 gigabit Ethernet. The Ethernet capabilities in OS X include the following

Automatic link detection.

Automatic link detection brings up the network stack whenever a cable is plugged in, and safely tears it down when the cable is removed.

Auto-MDIX

This feature reconfigures the connection depending on whether you are connecting to a router or another computer, so you no longer need special crossover cables.

Autonegotiation

Autonegotiation discovers and uses the appropriate transmission parameters for a given connection, such as speed and duplex matching.

Channel bonding

Channel bonding supports the IEEE 802.3ad/802.1ax Link Aggregation Control Protocol for using multiple low-speed physical interfaces as a single high-speed logical interface.

Jumbo frames

This capability uses Ethernet frames of up to 9000 bytes with Gigabit Ethernet switches that allow them.

TCP segmentation offload

To reduce the work required of the CPU, TCP segmentation offload lets the Network Interface Card (NIC) handle splitting a large outgoing buffer into individual packets.

Wi-Fi

Apple brought Wi-Fi to the mass market with the original Airport card and continues to provide cutting edge wireless networking across our product lines.

Built in to every Mac

Every Mac we ship—from the 11-inch Macbook Air to the top-of-the-line Mac Pro—has 802.11n networking built right in, along with 802.11a/b/g compatibility.

AirDrop

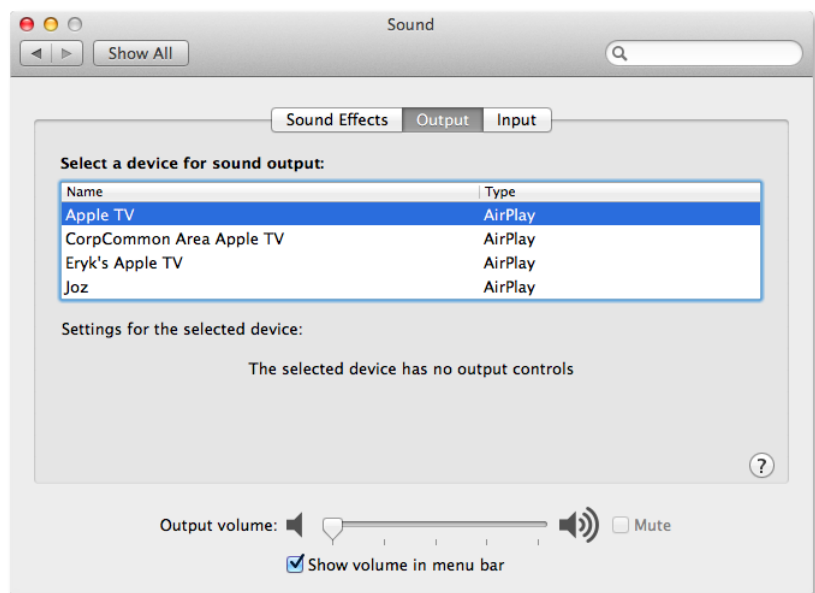
AirDrop, introduced in OS X 10.7 Lion, makes it easy to safely share files wirelessly with nearby users, even if you aren't on the same network. AirDrop leverages the wireless hardware on newer Mac systems to find and connect to other computers on an ad hoc basis, even if they are already associated with different Wi-Fi networks.



Share files wirelessly with anyone around you using AirDrop.

AirPlay

AirPlay lets you stream music throughout your entire house—wirelessly. Starting with OS X 10.8 Mountain Lion, you can share audio or mirror your screen from your Mac to an Apple TV or any other AirPlay-enabled device.



OS X treats AirPlay as just another audio output device.

Multihoming

OS X can have multiple network interfaces active at the same time and dynamically determines the optimal one to use for a given connection. Here are some examples of where this is useful:

- Connecting to the Internet via Ethernet when you plug a Mac in to the network, but seamlessly switching over to Wi-Fi when the network cable is unplugged.
- Routing all corporate traffic through a VPN server for security, while accessing the public Internet directly to reduce latency.
- Internet Sharing, where one interface, such as Ethernet, is connected to the public Internet while the other, such as Wi-Fi, acts as a router for connecting your other devices.

IPv6

OS X provides best-of-breed support for IPv6, the next-generation 128-bit Internet protocol.

Key features of IPv6 in OS X include:

- Full support for both stateful and stateless DHCPv6
- Happy Eyeballs algorithm ([RFC 6555](#)) for intelligently selecting between IPv6 and IPv4 addresses when both are available
- High-level APIs that resolve names directly so applications don't need to know whether they are using IPv4 or IPv6
- IPv6-enabled user applications (for example, Safari)

Remote Access

Captive networks

Like iOS, OS X now automatically detects the presence of a captive network and prompts for the authentication necessary to reach the public Internet.

VPN client

OS X includes a virtual private network (VPN) client that supports the Internet standard Layer 2 Tunneling Protocol (L2TP) over IPSec (the secure version of IPv4), as well as the older Point-to-Point Tunneling Protocol (PPTP). OS X also includes a VPN framework developers can use to build additional VPN clients.

Firewalls

In addition to the `ipfw2`-based system-wide firewall, OS X includes an application firewall that can be configured to allow only incoming access to preapproved applications and services.

Self-tuning TCP

OS X sets the initial maximum TCP window size according to the local resources and connection type, enabling TCP to optimize performance when connecting to high-bandwidth/high-latency networks.

Port mapping

NAT-PMP enables you to export Internet services from behind a NAT gateway, while Wide Area Bonjour lets you register the resulting port number with Back to My Mac. This enables you to easily and securely access your home printer and disk drives remotely, even from the public Internet.

Bonjour

Bonjour is Apple's implementation of the Zero Configuration Networking standard. It helps applications discover shared services such as printers on the local network. It also enables services to coordinate within and across machines without requiring well-known port numbers. Bonjour's ability to painlessly find other computers over a network is critical to many Apple technologies, such as AirPlay and AirDrop.

Link-local addressing

Any user or service on a computer that needs an IP address benefits from this feature automatically. When your host computer encounters a local network that lacks DHCP address management, it finds an unused local address and adopts it without you having to take any action.

Multicast DNS

Multicast DNS (mDNS) uses DNS-format queries over IP multicast to resolve local names not handled by a central DNS server. Bonjour goes further by handling mDNS queries for any network service on the host computer. This relieves your application of the need to interpret and respond to mDNS messages. By registering your service with the Bonjour mDNSResponder daemon, OS X automatically directs any queries for your name to your network address.

Service discovery

Service discovery allows applications to find all available instances of a particular type of service and to maintain a list of named services. The application can then dynamically resolve a named instance of a service to an IP address and port number. Concentrating on services rather than devices makes the user's browsing experience more useful and trouble-free.

Wide Area Bonjour

Starting in OS X 10.4, Bonjour now uses Dynamic DNS Update ([RFC 2316](#)) and unicast DNS queries to enable discovery and publishing of services to a central DNS server. These can be viewed in the Bonjour tab of Safari in addition to other locations. This feature can be used by companies to publicize their Intranet or by retailers to advertise promotional web sites.

High-level APIs

OS X provides multiple APIs for publication, discovery, and resolution of network services, as follows:

- NSNetService and NSNetServiceBrowser classes, part of the Cocoa Foundation framework, provide object-oriented abstractions for service discovery and publication.
- The CFNetServices API declared in the Core Services framework provide Core Foundation-style types and functions for managing services and service discovery.
- The DNS Service Discovery API, declared in `</usr/include/dns_sd.h>`, provides low-level BSD socket communication for Bonjour services.

Wake On Demand

Wake on Demand allows your Mac to sleep yet still advertise available services via a Bonjour Sleep Proxy (typically an AirPort Extreme Base Station) located on your network. The proxy automatically wakes your machine when clients attempt to access it. Your Mac can even periodically do a maintenance wake to renew its DHCP address and other leases.

Open source

The complete Bonjour source code is available under the [Apache License, Version 2.0](#) on Apple's open source website, where it's called the [mDNSResponder](#) project. You can easily compile it for a wide range of platforms, including UNIX, Linux, and Windows. We encourage hardware device manufacturers to embed the open source mDNSResponder code directly into their products and, optionally, to pass the [Bonjour Conformance Test](#) so they can participate in the [Bonjour Logo Licensing Program](#).

Document Lifecycle

Auto Save

You no longer need to manually save important documents every few minutes, thanks to the new Auto Save facility introduced in OS X 10.7 Lion. Applications that support Auto Save automatically save your data in the background whenever you pause or every five minutes, whichever comes first. If the current state of your document has been saved, OS X won't even prompt you before quitting the application, making logouts and reboots virtually painless.

Automatic Versions

Versions, also introduced in OS X 10.7 Lion, automatically records the history of a document as you create and make changes to it. OS X automatically creates a new version of a document each time you open it and every hour while you're working on it. You can also manually create snapshots of a document whenever you like.

OS X uses a sophisticated chunking algorithm to save only the information that has changed, making efficient use of space on your hard drive (or iCloud). Versions understands many common document formats, so it can chunk documents between logical sections, not just at a fixed number of bytes. This allows a new version to store—for example, just the one chapter you rewrote instead of a copy of the entire novel.

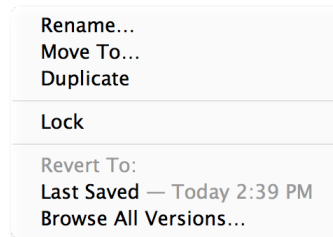
OS X automatically manages the version history of a document for you, keeping hourly versions for a day, daily versions for a month, and weekly versions for all previous months.

To further safeguard important milestones, OS X automatically locks documents that were edited more than two weeks ago. You can change the interval by clicking the Options... button in the Time Machine System Preferences pane, then choosing the interval you want from the Lock documents pop-up menu.

When you share a document—for example through email, iChat, or AirDrop—only the latest, final version is sent. All other versions and changes remain safely on your Mac.

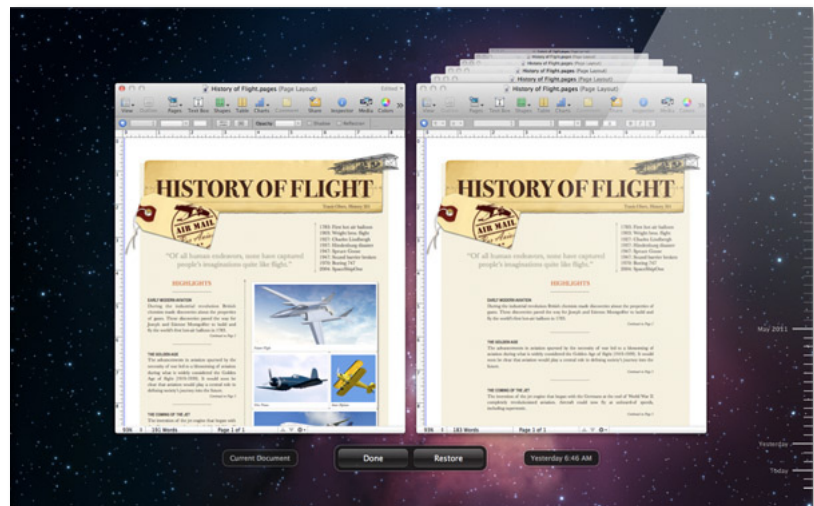
Version Management

You can also manually lock, unlock, rename, move, or duplicate documents using the pop-up menu next to the document title, which also shows you the current state of the document.



Manage your versions directly from the pop-up menu next to the document title.

You can also use the same pop-up menu to browse previous versions using an interface similar to Time Machine. It shows the current document next to a cascade of previous versions, letting you make side-by-side comparisons. You can restore entire past versions or bring elements from past versions such as pictures or text into your working document.



Recovering work from previous versions is just a click away.

iCloud Storage

iCloud Storage APIs enable apps to store documents and key value data in iCloud. iCloud wirelessly pushes documents to your devices and updates them whenever any of your devices change them—all automatically.

Ubiquitous storage

The iCloud storage APIs let applications write your documents and data to a central location and access those items from all your computers and iOS devices. Making a document ubiquitous using iCloud means you can view or edit those documents from any device without having to sync or transfer files explicitly. Storing documents in your iCloud account also provides an extra layer of protection. Even if you lose a device, those documents are still available from iCloud storage.

File coordination

Because the file system is shared by all running processes, conflicts can occur when two processes (or two threads in the same process) try to change the same file at the same time. To avoid this type of contention, OS X 10.7 and later include support for file coordinators, which enable developers to safely coordinate file access between different processes or different threads.

File coordinators mediate changes between applications and the daemon that facilitates the transfer of the document to and from iCloud. In this way, the file coordinator acts as a locking mechanism for the document, preventing applications and the daemon from modifying the document simultaneously.

Safe versions

Versions automatically stores iCloud documents. This means iCloud never asks you to resolve conflicts or decide which version to keep. It automatically chooses the most recent version. You can always use the Browse Saved Versions option if you want to revert to a different one. Versions' chunking mechanism also minimizes the information that needs to be sent across the network.

Ubiquitous metadata, lazy content

iCloud immediately updates the metadata (that is, the file name and other attributes) for every document stored or modified in the cloud. However, iCloud may not push the actual content to devices until later, perhaps only when actively requested. Devices always know what's available but defer loading the data in order to conserve storage and network bandwidth..

Peer-to-peer networking

iCloud detects when you have multiple devices on the same local network, and it copies the content directly between them rather than going through the cloud. It eventually copies the content to the cloud, as well, to enable remote access and backup.

Web access

iCloud provides a range of powerful web applications to let you work directly with your data from a web browser. These include the usual personal information tools (Mail, Calendar and AddressBook) as well as a complete suite of iWork viewers (Pages, Keynote, and Numbers).

Data Management

Spotlight

Spotlight is a fast desktop search technology that helps you organize and search for files based on either contents or metadata. It's available to users via the Spotlight window in the upper-right of the screen. Developers can embed Spotlight in their own applications using an API available from Apple.

Standard metadata

Spotlight defines standard metadata attributes that provide a wide range of options for consistently storing document metadata, making it easier to form consistent queries. These include POSIX-style file attributes, authoring information, and specialized metadata for audio, video, and image file formats.

Extensible importers

Using OS X Launch Services, Spotlight determines the uniform type identifier of a new or modified file and attempts to find an appropriate importer plug-in. If an importer exists and is authorized, OS X loads it and passes it the path to the file.

Third parties can create custom importers that extract both standard and custom metadata for a given file type and return a dictionary which is used to update the Spotlight datastore.

Dynamic datastore

Every time you create, modify, or delete a file, the kernel notifies the Spotlight engine that it needs to update the system store. OS X accomplishes this with the high-performance `fs_events` API.

Live update

Whenever OS X updates the datastore, it also notifies the system results window and any third-party client applications if the update causes different files to match or not match the query. This ensures that the Mac always presents the latest real-time information to the user.

Time Machine

Time Machine, introduced in OS X 10.5 Leopard, makes it easy to back up and restore either your entire system or individual files.

Easy setup

To set up Time Machine, all you need to do is select a local disk or Time Capsule to store the backups. In OS X Mountain Lion, you can select multiple backup destinations for Time Machine. OS X immediately starts backing up all your files in the background. After the initial backup, it automatically creates new incremental backups every hour.

Coalescing changes

Time Machine leverages the `fsevents` technology developed for Spotlight to continuously identify and track any folders (what UNIX calls *directories*) that contain modified files. During the hourly backup, it creates a new folder that appears to represent the entire contents of your hard drive. In reality, it uses a variant of UNIX hard links that mostly point to trees of unmodified folders already on the disk. Those trees are effectively copy-on-write, so that future changes never affect the backup version.

Time Machine creates new trees inside a backup for any path that contains modified folders. Time Machine creates new versions of those folders that contain links to the current files, thus automatically capturing any changes that occurred in the past hour. This avoids the overhead of either scanning every file on disk or capturing each and every change to a file.

This technique allows each backup to provide the appearance and functionality of a full backup while only taking up the space of an incremental backup (plus some slight overhead for the metadata of modified trees). This makes it easy to boot or clone a system from the most recent Time Machine backup.

Mobile Time Machine

OS X 10.7 Lion introduced Mobile Time Machine, which keeps track of modified files even while you are disconnected from your backup drive. When you reconnect, it will automatically record the hourly snapshots to ensure you don't lose your version history.

Preserving backups

Time Machine keeps hourly backups for the past 24 hours, daily backups for the past month, and weekly backups until your backup drive is full. At that point OS X warns you that it is starting to delete older backups. To be notified whenever OS X deletes an older backup, open Time Machine preferences, click the Options... button, and check the box next to Notify after old backups are deleted.

Developer Tools

LLVM

The next-generation LLVM compiler suite is based on the open source LLVM.org project. The LLVM.org project employs a unique approach of building compiler technologies as a set of libraries. Capable of working together or independently, these libraries enable rapid innovation and provide the ability to attack problems never before solved by compilers.

Apple's compiler, runtime, and graphics teams are extensive contributors to the LLVM.org community. They use LLVM technology to make Apple platforms faster and more secure.

Clang front-end

Clang is a high-performance front-end for parsing C, Objective-C, and C++ code as part of the LLVM compiler suite. It supports the latest C++ standards, including a brand-new implementation of the C++ standard libraries. Clang is also implemented as a series of libraries, allowing its technology to be reused for [static code analysis](#) in Xcode and the [LLDB debugger](#).

Comprehensive optimization

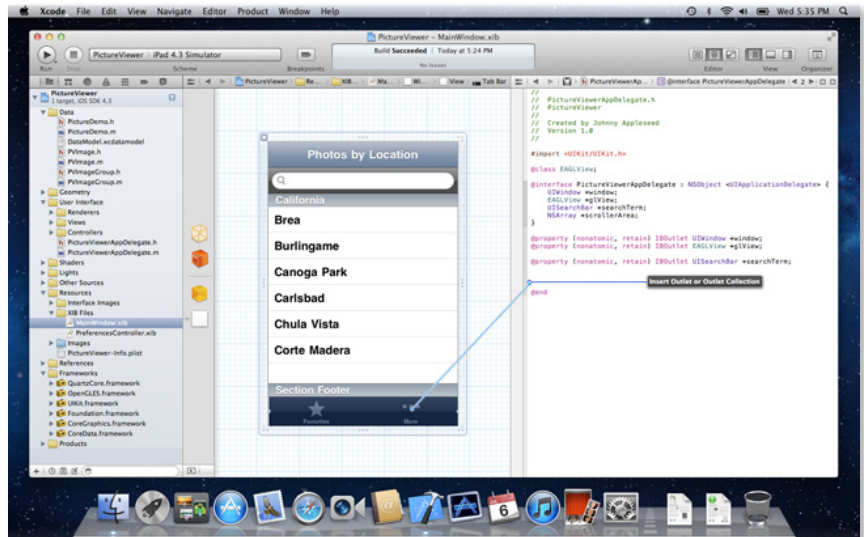
LLVM's flexible architecture makes it easy to add sophisticated optimizations at any point during the compilation process. For example, LLVM performs whole-program analysis and link-time optimizations to eliminate unused code paths.

Automatic Reference Counting

Automatic Reference Counting (ARC) for Objective-C lets the compiler take care of memory management. By enabling ARC with the new Apple LLVM compiler, you never need to manually track object lifecycles using `retain` and `release`, dramatically simplifying the development process while reducing crashes and memory leaks. The compiler has a complete understanding of your objects and releases each object the instant it is no longer used. Apps run as fast as ever, with predictable, smooth performance.

Xcode

Xcode 4 is the latest version of Apple's integrated development environment (IDE), a complete toolset for building OS X and iOS applications. The Xcode IDE includes a powerful source editor, a sophisticated graphical UI editor, and many other features from highly customizable builds to support for source code repository management. Xcode can help you identify mistakes in both syntax and logic and will even suggest fixes.



The Xcode 4 integrated development environment

Static analysis

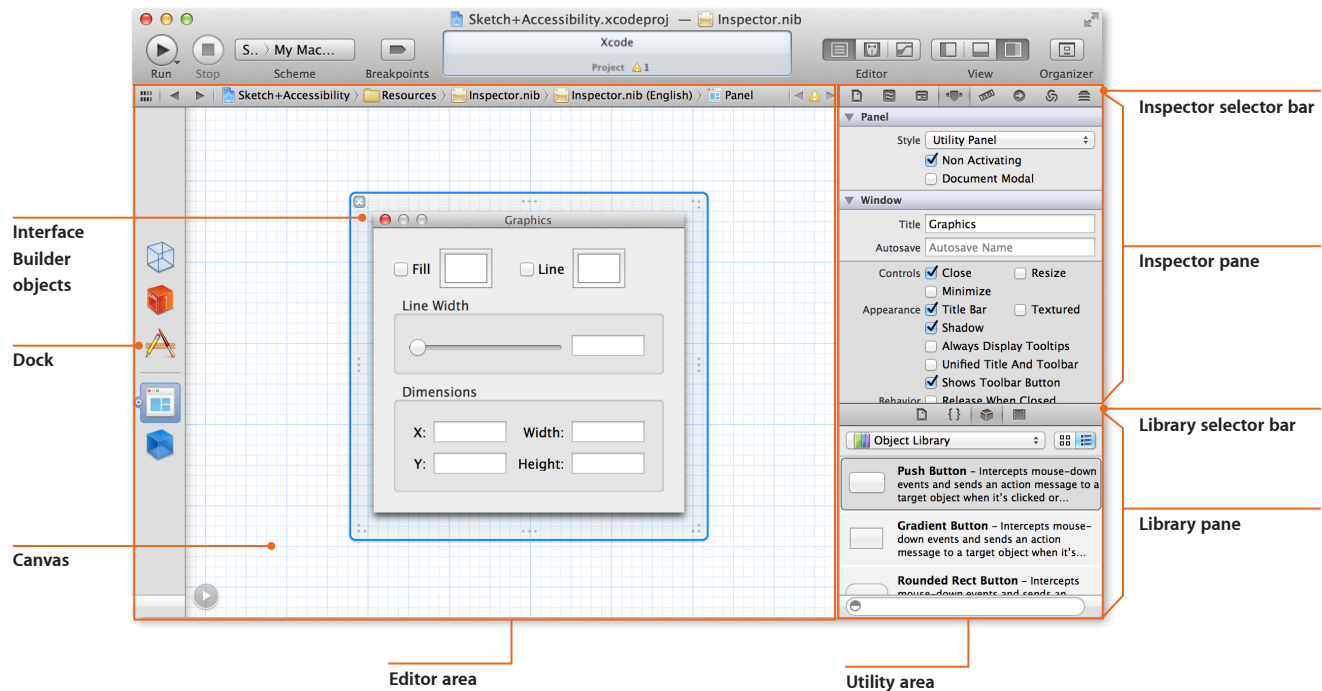
You can think of static analysis as providing you advanced warnings by identifying bugs in your code before it is run—hence the term *static*. The Xcode static analyzer gives you a much deeper understanding of your code than do traditional compiler warnings. The static analyzer leverages the Clang libraries to travel down each possible code path, identifying logical errors such as unreleased memory—well beyond the simple syntax errors normally found at compile time.

Fix-it

Fix-it brings autocorrection from the word processor to your source code. The Xcode Fix-it feature checks your symbol names and code syntax as you type, highlights any errors it detects, and even fixes them for you. Fix-it marks syntax errors with a red underbar or a caret at the position of the error and a symbol in the gutter. Clicking the symbol displays a message describing the possible syntax error and, in many cases, offers to repair it automatically.

Interface Builder

Interface Builder is a graphical tool for designing user interfaces for OS X and iOS applications. Like other Xcode editors, Interface Builder is fully integrated into the application, so you can write and edit source code and tie it directly to your user interface without leaving the Xcode workspace window.



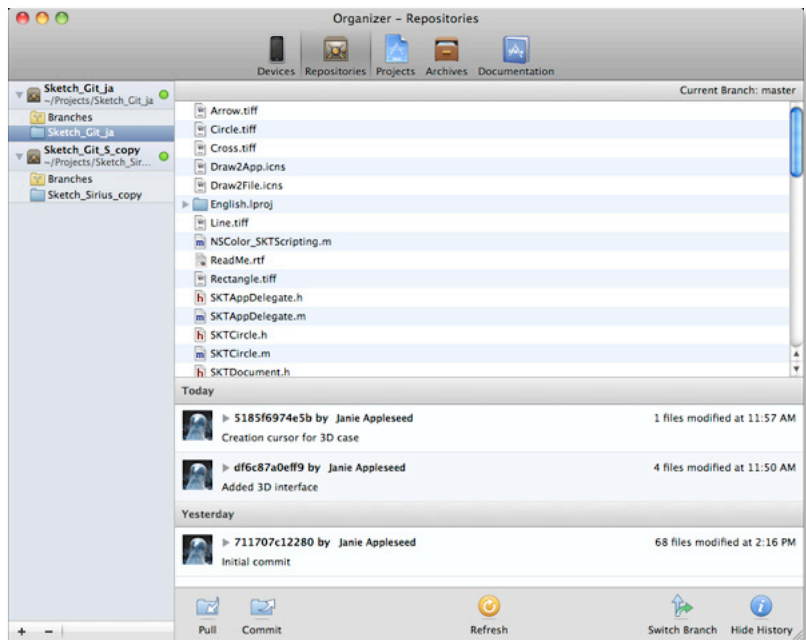
Interface Builder, the easiest way to design your application's user interface.

Version control

Xcode provides several ways to save versions of your project:

- A snapshot saves the current state of your project or workspace on disk for possible restoration later.
- Source control repositories keep track of individual changes to files and enable you to merge different versions of a file.
- An archive packages your products for distribution, either through your own distribution mechanism or for submission to the App Store.

Xcode also provides direct support for Git and Subversion repositories, including an option to create a local Git repository when you create a new project. Because it's so easy to set up a repository to use with your Xcode project, Xcode provides a special editor, called the version editor, that also makes it easy to compare different versions of files saved in repositories.

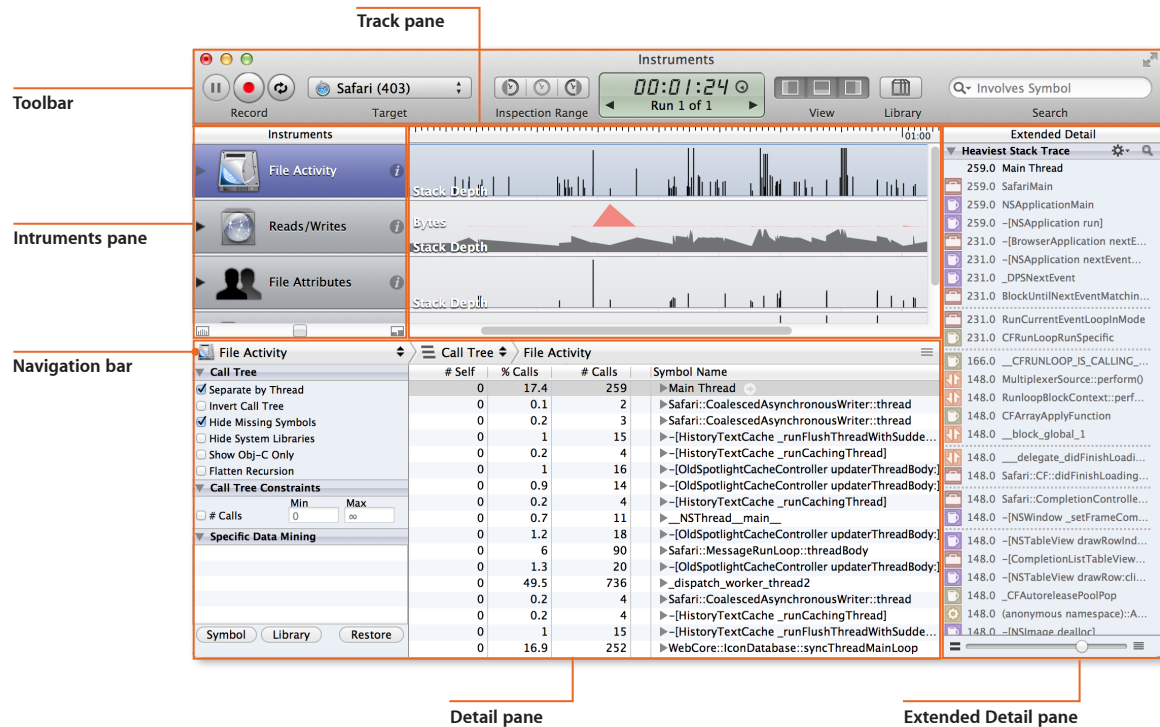


The Xcode version editor.

Instruments

Instruments is an application for dynamically tracing and profiling OS X and iOS code. It is a flexible and powerful tool that lets you track one or more processes, examine the collected data, and track correlations over time. In this way, Instruments helps you understand the behavior of both user programs and the operating system.

With the Instruments application, you use special tools (known as instruments) to trace different aspects of a process's behavior. You can also use the application to record a sequence of user interface actions and replay them, using one or more instruments to gather data.



Instruments includes Instruments, Track, and Extended Detail panes.

Synchronized tracks

The Instruments Track pane displays a graphical summary of the data returned by the current instruments. Each instrument has its own track, which provides a chart of the data collected by that instrument. The information in this pane is read-only. You use this pane to select specific data points you want to examine more closely.

Multiple traces

Each time you click the Record button in a trace document, Instruments starts gathering data for the target processes. Rather than appending the new data to any existing data, Instruments creates a new trace run to store that data. This makes it easy to compare behavior between different configurations.

A trace run consists of all of the data gathered between the time you click the Record button and the Stop button. By default, Instruments displays only the most recent trace run in the Track pane, but you can view data from previous trace runs in one of two ways:

- Use the Time/Run control in the toolbar to select which trace run you want to view.
- Click the disclosure triangle next to an instrument to display the data for all trace runs for that instrument.

User interface recording

A user interface track records a series of events or operations in a running program. After the track records events, you can replay that track multiple times to reproduce the same sequence of events over and over. Each time you replay a user interface track, you can collect data using other instruments in your trace document. The benefit of doing this is that you can then compare the data you gather on each successful run and use it to measure the changes in your application's performance or behavior.

DTrace

DTrace is a dynamic tracing facility available for Mac systems since OS X 10.5 Leopard. Because DTrace taps into the operating system kernel, you have access to low-level information about the kernel itself and about the user processes running on your computer. DTrace is used to power many of the built-in instruments.

DTrace probes make it easy to use Instruments to create custom instruments. A probe is a sensor you place in your code that corresponds to a location or event (such as a function entry point) to which DTrace can bind. When the function executes or the event is generated, the associated probe fires and DTrace runs whatever actions are associated with the probe.

Most DTrace actions simply collect data about the operating system and user program behavior at that moment. It is possible, however, to run custom scripts as part of an action. Scripts let you use the features of DTrace to fine tune the data you gather. That data is then available as an Instruments track to compare with data from other instruments or other trace runs.

Accelerate

Accelerate is a unique framework of hardware-optimized math libraries that provides the following:

- Vector digital signal processing (vDSP). Optimized Fast Fourier Transforms (FFTs), convolutions, vector arithmetic, and other common video and audio processing tasks for both single- and double-precision data.
- Vector image processing (vImage). Optimized routines for convolutions, compositing, color correction, and other image-processing tasks, even for gigapixel images.
- vForce. Designed to wring optimal efficiency from modern hardware by specifying multiple operands at once, allowing only default IEEE-754 exception handling.
- Linear Algebra Package (LAPACK). Industry-standard APIs written on top of BLAS for solving common linear algebra problems.
- Basic Linear Algebra Subprograms (BLAS) Levels I, II, and III. High-quality "building block" routines that perform basic vector and matrix operations using standard APIs.
- vMathLib. A vectorized version of libm that provides transcendental operations, enabling you to perform standard math functions on many operands at once.

Automation

AppleScript

AppleScript is Apple's native language for application automation, as used by the AppleScript Editor. Its English-like syntax generates Apple events, which use a scripting dictionary (provided by most Mac applications) to programmatically create, edit, or transform their documents. AppleScript and other Open Scripting Architecture (OSA) scripts can be activated by contextual menus, user interface elements, iCal events, and even folder actions, such as drag and drop.

Automator

Automator provides a graphical environment for assembling actions (typically built from AppleScript or shell scripts) into sophisticated workflows, which can be saved as either standalone applications or as custom services, print plugins, folder actions, iCal alarms, and Image Capture plugins.

Apple events

The Apple Event Bridge framework provides an elegant way for Cocoa applications (including bridged scripting languages) to generate Apple events based on an application's dictionary, even generating appropriate header files if necessary.

Services

The Services menu lets you focus on only those actions relevant to your current selection, whether in the menu bar, the Finder action menu, or a contextual menu. Individual services can also be disabled and assigned shortcuts from the Keyboard pane in System Preferences.

WebKit

WebKit is an open source web browser engine developed by Apple. WebKit's HTML and JavaScript code began as a branch of the [KHTML](#) and [KJS](#) libraries from [KDE](#).

WebKit is also the name of the OS X system framework version of the engine that's used by [Safari](#), Dashboard, Mail, and many other OS X applications

Key features include:

- Lightweight footprint
- Great mobile support
- Rich HTML5 functionality
- Easy to embed in Cocoa and Cocoa touch applications
- Available as open source at webkit.org

For More Information

- Extensible Firmware Interface (EFI): See www.uefi.org
- I/OKit: See [Kernel Programming Guide: I/O Kit Overview](#)
- Partition Schemes: See [Technical Note TN2166: Secrets of the GPT](#)
- Recovery Partitions: See [OS X Lion: About Lion Recovery](#).
- Full-Disk Encryption: See [OS X Lion: About FileVault 2](#).
- Backup: See [Mac 101: Time Machine](#).
- File System Events: See [Spotlight Overview](#)
- Launchd: See the [Daemons and Services Programming Guide](#)
- Grand Central Dispatch (GCD): See the [Concurrency Programming Guide](#)
- Sandboxes: See [Code Signing Guide](#)
- Gatekeeper: See [Distributing Outside the Mac App Store](#)
- Bonjour: See [Bonjour Overview](#).
- XPC: See [Daemons and Services Programming Guide: Creating XPC Services](#).
- iCloud: See [What's New In OS X: iCloud Storage APIs](#)
- LLVM: See [The LLVM Compiler Infrastructure Project](#)
- Xcode: See [Xcode 4 User Guide](#)
- Instruments: See [Instruments User Guide](#)
- WebKit: See [WebKit Objective-C Programming Guide](#).

For More Information

For more information about OS X Mountain Lion, visit www.apple.com/macosx.

© 2012 Apple Inc. All rights reserved. Apple, the Apple logo, AirPlay, Airport, AirPort Extreme, Apple TV, AppleScript, Back to My Mac, Bonjour, Cocoa, iCloud, MacBook, MacBook Air, Mac Pro, OS X, Safari, Spotlight, Time Machine, and Xcode are trademarks of Apple Inc., registered in the U.S. and other countries. AirDrop and Open CL are trademarks of Apple Inc. App Store and iTunes Store are service marks of Apple Inc., registered in the U.S. and other countries. Intel, Intel Core, and Xeon are trademarks of Intel Corp. in the U.S. and other countries. UNIX® is a registered trademark of The Open Group. Other product and company names mentioned herein may be trademarks of their respective companies. June 2012 L516500A