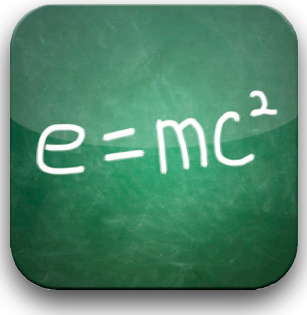
iOS 5 Education
Deployment Guide

Contents

iOS in Education **3**
System Requirements **5**
Preparing for Deployment **6**
Preparing a Staging Area 6
Understanding Firewall Requirements 6
Discovering Apps for Learning 6
Contacting Apple 6
AppleCare 6
Apple Professional Services 7
Apple Factory Services 9
Apple Professional Development 9
Wi-Fi Network Design **11**
Planning for Coverage and Density 11
Apple iPad Learning Labs 13
Supporting AirPlay, AirPrint, and iTunes Wi-Fi Sync 14
Configuration and Management **15**
Manually Configuring Devices 15
Understanding Configuration Profiles 15
Using Mobile Device Management Solutions 16
Using Exchange ActiveSync 18
Purchasing Content **19**
Purchasing with a Credit Card or iTunes Gift Card 19
Volume Purchase Program 19
Understanding Program Roles 20
Enrolling in the Volume Purchase Program 21
Understanding Volume Vouchers 21
Using the Volume Purchase Program 21
Volume Pricing 22
Code Distribution Techniques 22
Deployment Strategies **23**
Understanding iTunes 23
Managing Documents 24
Deployment Models 25
Personal Ownership Model 25
Institutional Ownership Model 26
Layered Ownership Model 33
Choosing a Deployment Strategy 35
Other Options 36
Troubleshooting Resources 37
Summary **38**

iOS in Education

Learn how to deploy and support iOS devices in an education environment.



This guide is designed for those responsible for the deployment of iOS devices, from IT leadership to implementors. It highlights best practices and considerations relevant to deploying and supporting iOS devices in education environments.

Note: Curriculum design is outside the scope of this document.

It's important to develop and communicate a plan before you deploy devices. Early design decisions, both good and bad, are amplified as a deployment is scaled up. Curriculum and technology leadership as well as those who will implement the design should be included in the planning process. A well-planned iOS deployment will likely incorporate some version of the following steps:

1. Understand the deployment goals.
   - What are the expected outcomes?
2. Assess the infrastructure.
   - Can the LAN and Wi-Fi network support high density of devices?
   - Review server and storage design (local or hosted).
   - Evaluate Internet bandwidth.
3. Plan for support.
   - Will Apple provide project management support from Apple Professional Services?
   - Who will be responsible for post-deployment support?
   - Will Apple provide professional development for implementors?
4. Plan the rollout.
   - What policies need to be created or revised?
   - Who will get devices and in what order will they be distributed?
   - Will Apple provide professional development for instructors and administrators?
   - What is the training plan for students?
   - Who will be authorized to purchase apps?
   - What data needs to be backed up from iOS devices?
   - Which deployment strategies will be used?
   - Will Apple Professional Services execute the rollout?
   - Enroll in the Volume Purchase Program.
   - Consider a Mobile Device Management solution.
5. Execute the purchase.
   - Order the iOS devices, accessories, and related equipment.
   - Purchase apps in volume using the Volume Purchase Program.

6. Prepare for rollout.
   - Prepare a secure space for unpacking devices, activation, and the initial sync.
   - Configure sync stations, carts, and iOS devices.
7. Perform the initial rollout.
   - Deploy to initial sites.
   - Verify the deployment model.
8. Communicate with stakeholders (the School Board, Board of Trustees, community, and so on).
   - Describe and explain the deployment plan.
   - Reiterate expected outcomes.
9. Scale up the deployment.
   - Expand to remaining sites using best practices.
10. Verify.
    - Collect data and verify deployment fidelity.

This document focuses on the technical aspects of the steps listed above. Many curriculum resources are available for help with designing classroom workflows for iOS devices.

- Learn more about iPad in education
  www.apple.com/education/ipad
- Learn more about iPod touch and iPhone in education
  www.apple.com/education/ipodtouch-iphone
- Find education resources, video tutorials, and other guides
  www.apple.com/education/resources

System Requirements

The following resources are where you can find information about the operating system versions and related software that are required to follow the recommendations in this document.

iPhone, iPad, and iPod touch

- Learn more about iPhone system requirements
  www.apple.com/iphone/specs.html
- Learn more about iPad system requirements
  www.apple.com/ipad/specs
- Learn more about iPod touch system requirements
  www.apple.com/ipodtouch/specs.html
- Learn more about Apple TV system requirements
  www.apple.com/appletv/specs.html
- Learn more about the latest version of iOS
  www.apple.com/ios

iPhone Configuration Utility

- Learn more about iPhone Configuration Utility system requirements
  www.apple.com/support/iphone/enterprise

iTunes

- Learn more about iTunes system requirements
  www.apple.com/itunes/download

OS X Lion Server

- Learn more about OS X Lion Server system requirements
  www.apple.com/macosx/server/specs.html

Preparing for Deployment

Strategic preparation prior to deployment can facilitate a smooth rollout. This chapter discusses key preparation options.

Preparing a Staging Area

Before any equipment arrives, it is helpful to reserve and prepare an appropriate workspace for the deployment. Devices may need to be configured and inventoried before their delivery to end users, so consider designating a secure location for equipment that has adequate power and networking support.

Understanding Firewall Requirements

Confirm that the appropriate firewall ports are open before proceeding with the tasks discussed in this guide. It is also useful to understand what ports iTunes and iOS devices use for various services.

- Learn about well-known TCP and UDP ports used by Apple
  http://support.apple.com/kb/TS1629
- Learn about Apple TV firewall requirements
  http://support.apple.com/kb/HT2463

Discovering Apps for Learning

Consider doing research about apps before devices arrive for a more efficient deployment. Instructors new to iOS may appreciate having a starting point as they choose an app for a specific content area.

- Learn about great learning apps
  www.apple.com/education/apps

Contacting Apple

To learn more about Apple in education, visit www.apple.com/education or call 800-800-2775 to speak to an Apple education representative.

AppleCare

AppleCare products are available for institutions of every size.

AppleCare Protection Plan for iPhone, iPad, or iPod touch

Every iPhone, iPad, and iPod touch comes with complimentary telephone technical support for 90 days from purchase and a one-year limited warranty. With the AppleCare Protection Plan, the service coverage can be extended to two years from the original purchase date. You can call Apple's technical support experts as often as you like and get questions answered. There are convenient service options if repair service is needed.

- Learn more about AppleCare Protection Plan for iPhone
  www.apple.com/support/products/iphone.html

- Learn more about AppleCare Protection Plan for iPad
  www.apple.com/support/products/ipad.html
- Learn more about AppleCare Protection Plan for iPod touch
  www.apple.com/support/products/ipod.html

AppleCare iOS Direct Service Program

A benefit of the AppleCare Protection Plan, the iOS Direct Service Program screens the units for any hardware faults and, if necessary, directly orders a replacement iPhone, iPad, iPod touch, or in-box accessory, and exchanges it for the failed item at their service location. This provides convenience and cost reduction to organizations. The program is open to businesses/enterprise organizations, education institutions, and U.S., state, and local government agencies.

- Learn more about the iOS Direct Service Program
  www.apple.com/support/programs/ids

AppleCare Help Desk Support

AppleCare Help Desk Support provides priority access to Apple's senior technical support staff by telephone. It also includes a suite of tools to diagnose and troubleshoot Apple hardware, allowing institutions to manage resources more efficiently, improve response time, and reduce training costs. AppleCare Help Desk Support covers an unlimited number of support incidents for hardware and software diagnosis and troubleshooting and issue isolation for Apple-based solutions such as iPhone, iPad, iPod touch, iPhone Configuration Utility, and iOS.

- Learn more about AppleCare Help Desk Support
  www.apple.com/support/products/enterprise/help.html

AppleCare OS Support

AppleCare OS Support includes AppleCare Help Desk Support in addition to enterprise-level incident support—defined as support for system components, network configuration and administration, integration into heterogeneous environments, professional software applications, web applications and services, and technical issues requiring the use of the command-line tools for resolution.

- Learn more about AppleCare OS Support
  www.apple.com/support/products/enterprise/server.html

Learn More

- For more information about AppleCare, see the *Contacting Apple* section of this chapter.

Apple Professional Services

Apple Professional Services experts are among the industry's most experienced and respected. Drawing on decades of experience in education as well as industry certification training, Apple Professional Services helps you leverage your technology investments to make an educational difference.

Apple Professional Services has a complete array of offerings to meet the diverse needs of education institutions, including K-12 schools, school district offices, and universities. Here are a few examples of what Apple Professional Services can help with:

- Assessing, planning, managing, delivering, and supporting a fully mobile learning environment

- Deploying supplemental services for mobile collaboration, communication, and learning
- Creating a new campus-wide technology solution or integrating Apple technology with your existing systems
- Mentoring technical staff and educators so they get the most out of the iOS deployment

In addition to offering solutions for integrating iPhone, iPad, and iPod touch into an education infrastructure, Apple Professional Services can also show you how iOS devices like iPad and iPod touch can transform learning.

Apple Configuration Services

Educational technology deployments require detailed coordination and technical expertise to minimize risk and ensure success. Apple project managers provide coordination and oversight of an entire deployment process from project scope, scheduling, and communications to staging, syncing, and deployment. Apple's expertise in managing these detailed logistics reduces your risk by ensuring timely, successful deployments that meet your educational goals as well as your budget.

Having highly-skilled, experienced engineers assist with an iOS device deployment can help ensure a well-designed deployment. Apple Professional Services engineers work with you to design, plan, configure, and integrate iPad and iPod touch management and deployment strategies in a learning environment. These services are always designed to coach and mentor an organization on the specific deployment, helping staff build self-sufficiency.

Apple Deployment Services

When you're ready to deploy, Apple Deployment Services provides skilled and efficient technicians who apply asset tags, activate and set up the iOS devices, assemble mobile carts, and even remove all packing materials from your site.

Post-Deployment

Once the deployment is complete, Apple Professional Services can help with maintenance tasks of your solution: product cleaning and repair, new software configuration, remote assistance, regular reevaluation of the infrastructure, and planning for new faculty development and continuing IT skills development.

Getting Started with Integrating iPad and iPod touch

Apple Professional Services offers Getting Started solutions tailored to help with initial iPad and iPod touch deployments that include building configuration profiles and content libraries, activation, and synchronization. These customized solutions provide mentoring for IT staff and educators to ensure successful integration into your learning environment.

Learn More

- For more information about ordering Apple Professional Services, see the *Contacting Apple* section of this chapter.

Apple Factory Services

Before iOS devices are shipped, certain work can be completed at the factory. This can include placing asset tags on devices, text or logo laser engraving the back of each device, and more.

Learn More

- For more information about Apple factory service options, see the *Contacting Apple* section of this chapter.

Apple Professional Development

Apple Professional Development offers onsite workshops that range from one to eight days long. These hands-on workshops are tailored to a school's or district's specific needs and are designed to enable attendees to transform teaching and learning using Apple products.

All Apple Professional Development facilitators are educators themselves. That gives them a unique view: they know what's important in the classroom, so they can ensure that workshop participants learn about the institution's Apple products and how they can best serve the educators and students.

Apple Professional Development workshops are flexible, allowing multiple entry points for professional development. You may begin with any workshop category, depending on faculty needs. One-day workshops may be broken into two half-day sessions to accommodate a variety of faculty groupings. Workshops apply toward Continuing Education Units, accommodate 16–20 participants, and incorporate Common Core State Standards. Apple Professional Development is for institutional/group purchase only. After purchasing, discuss implementation options with an Apple Professional Development facilitator.

Available Workshops

Apple Professional Development workshops are offered in several categories including:

- **Start**

  Focused on technology skills, these foundational workshops help teachers become confident and comfortable integrating Apple products into their teaching strategies.

- **Learn**

  These workshops help teachers apply their skills with specific Apple products and learning activities in content areas to produce effective personal learning for their students.

- **Instruct**

  Focused on curricula design and instruction, these workshops help teachers embrace the range of Apple products in their practice.

- **Lead**

  These workshops for school and district leaders focus on issues important to success—visioning/planning, implementing/managing, and designing curricula.

- **Support**

  Support teachers beyond workshops with in-class or web coaching and mentoring, technology self-assessments, workshop series, and customized workshop development.

Learn More

- For more information about Apple Professional Development, see the *Contacting Apple* section in this chapter.

Wi-Fi Network Design

When preparing the Wi-Fi infrastructure for an iOS deployment, there are several factors to consider:

- Required coverage area
- Number and density of devices using the Wi-Fi network
- Types of devices and their Wi-Fi capabilities
- Types and amount of data being transferred
- Security requirements for accessing the wireless network
- Encryption requirements for data passing through the air

Although this list is not exhaustive, it represents some of the most relevant Wi-Fi network design factors.

This chapter may be helpful for network administrators who are responsible for their own deployments, and it may help facilitate discussions with Wi-Fi vendors to ensure an optimal Wi-Fi network design.

Reminder: This chapter focuses on Wi-Fi network design in the United States. This design may differ for other countries.

Planning for Coverage and Density

Although it is critical to provide Wi-Fi coverage where iOS devices will be used, it is also essential to plan for the density of devices in a given area.

Most modern, enterprise-class access points are capable of handling up to 50 Wi-Fi clients, although the user experience would likely be disappointing if a single access point had that many devices associated to it. The experience on each device depends on the available wireless bandwidth on the channel in use and the number of devices sharing the overall bandwidth. As more and more devices use the same access point, the relative network speed for those devices decreases. You should consider the expected usage pattern of the iOS devices as part of your Wi-Fi network design.

Designing for Coverage

To illustrate, consider the following scenario of a district office building with ten large offices and a conference room on each floor. Fifty employees equipped with MacBook Pro notebooks and iPad and iPhone devices are spread out over two stories. The MacBook Pro notebooks are plugged into Ethernet ports when not mobile, while iPad and iPhone devices frequently change locations.

The physical layout of the building encourages informal communication and collaboration. Employees may meet with other employees in conference rooms or in offices. As a result, employees move around the building with iPad and iPhone devices throughout the day, and some employees bring their MacBook Pro notebooks with them. The majority of network access comes from checking email, calendars, and Internet browsing.

In this scenario, Wi-Fi coverage is the highest priority. These mobile users aren't likely to be transferring large amounts of data over the network very often, and the overall density of Wi-Fi devices is somewhat low. A Wi-Fi design could include two or three access points on each floor to provide coverage for the offices and one access point in each conference room. The MacBook Pro notebooks and iPad devices both support 802.11n at 5GHz, so the access points could be configured for 802.11n at 5GHz. HD40 can be enabled to increase the throughput of MacBook Pro notebooks on the network.

- Learn more about Wi-Fi standards support, including specifications for Apple products, in *Appendix A—Wi-Fi Standards* at the end of this document.

Recall that the employees also use iPhone devices, so a 2.4GHz network must also be available. Because most modern access points support simultaneous dual frequencies, support for both 2.4GHz and 5GHz networks could be enabled. iPhone 4 supports 802.11n, but if other mobile devices don't support 802.11n, 802.11b/g may also need to be enabled.

Designing for Density

Contrast the district office scenario above with a high school that has 1000 students and 30 teachers in a two-story building. Every student has been issued an iPad, and every teacher has been issued both a MacBook notebook and an iPad. Each classroom holds approximately 35 students, and classrooms are adjacent to each other. Throughout the day, students conduct research on the Internet, watch curriculum videos, and copy files to and from a file server on the LAN.

The Wi-Fi network design for this scenario is more complex due to the higher density of mobile devices. Because each classroom has approximately 35 students with iPad devices at any given time during the school day, one access point per classroom could be deployed. Multiple access points should be considered for the common areas to provide adequate coverage. The actual number of access points for the common areas will vary, depending on the density of Wi-Fi devices in those spaces.

iPad is the most common device used in this school, so special attention should be given to that device's technical specifications. iPad supports 802.11n at both 2.4GHz and 5GHz. Therefore, the access points throughout the school should be configured for 802.11n at 5GHz. Although iPad doesn't benefit from channel bonding, MacBook does. However, in this high-density deployment in which the majority of devices do not support channel bonding, it may be best to leave channel bonding disabled. This allows for the deployment of more access points without reusing the same channel in nearby locations. With channel bonding enabled (each access point uses two channels), fewer total channels are available.

- Learn more about Wi-Fi standards support, including specifications for Apple products, in *Appendix A—Wi-Fi Standards* at the end of this document.

If devices that only support the 802.11b or 802.11g standards are required to participate on the network, the above design could be modified slightly. One option is to simply enable 802.11g/b if dual-band access points are being deployed. Another option is to provision one SSID using 802.11n at 5GHz for newer devices and a second SSID at 2.4GHz to support 802.11b and 802.11g devices. However, care should be taken to avoid creating too many SSIDs.

The use of hidden SSIDs should be avoided in either design scenario. It is harder for a Wi-Fi device to rejoin a hidden SSID than a broadcast SSID, and there's very little security benefit in hiding the SSID. Users tend to frequently change location along with their iOS devices, so hidden SSIDs may delay network association time.

- Learn more about Wi-Fi security in *Appendix B—Wireless Security* at the end of this document.

Note that the above network designs are hypothetical examples. The actual design for an environment will vary depending on the unique characteristics of the building, user workflows, the specific Wi-Fi devices, security considerations, and other factors. Collaborate with a Wi-Fi infrastructure provider to ensure an optimal design.

Apple iPad Learning Labs

An Apple iPad Learning Lab streamlines the management of classroom sets of iPad devices. Each lab can store, charge, and sync up to 30 iPad devices and has room for a MacBook computer. The cart rolls easily around campus, so multiple classes can benefit, and it can be locked to secure the devices when they're not in use. Instead of students visiting a lab, the lab is brought into the classroom.

Providing Wi-Fi for mobile carts can be more complex, depending on the infrastructure that already exists. There are two ways to design a Wi-Fi network for mobile learning labs: mounting fixed access points to handle the devices wherever they go or providing an access point that stays with the cart.

Note in which classrooms or other areas these mobile labs will be used. When designing a fixed Wi-Fi infrastructure for carts, design for both coverage and density to support the number of devices that may be brought into each of those areas. This may mean an access point per classroom or designated usage area.

If there isn't an existing Wi-Fi infrastructure or there isn't coverage in the designated areas, an access point may be installed on the cart, assuming an Ethernet port is available near the cart. If this is done, Wi-Fi is always be available where the devices are used.

Installing an access point on every cart can be a challenge if a fixed Wi-Fi infrastructure already exists. A well-designed Wi-Fi infrastructure will have channel usage balanced so that access points in close proximity don't interfere with each other. Transmit power settings will also be configured to minimize overlapping of coverage areas.

If a cart with an access point is moved into an area that is already covered by the fixed Wi-Fi infrastructure, it could cause significant interference in that area, especially if the 2.4GHz frequency is used on both the cart and fixed access points. If the existing Wi-Fi infrastructure operates exclusively on the 2.4GHz frequency, the access point on the cart should be configured to use the 5GHz frequency exclusively to avoid interference.

Consult a Wi-Fi network provider to determine the best strategy for Wi-Fi coverage for Apple iPad Learning Labs.

- Learn more about Apple mobile learning labs
  www.apple.com/education/labs

Similar challenges arise if users install their own access points. These access points may compete for channels with the fixed Wi-Fi infrastructure.

Supporting AirPlay, AirPrint, and iTunes Wi-Fi Sync

If AirPlay, AirPrint, or iTunes Wi-Fi Sync will be used as part of an iOS deployment, ensure that the Wi-Fi network design supports Bonjour traffic. These services use Bonjour for automatic discovery, which requires that communicating devices be on a single subnet with broadcast traffic enabled.

- Learn more about supporting Bonjour on Wi-Fi networks in *Appendix C—Supporting Bonjour* at the end of this document.
- Learn more about AirPlay
  http://support.apple.com/kb/HT4437
- Learn more about AirPlay Mirroring
  http://support.apple.com/kb/TS4085
- Learn more about AirPrint
  http://support.apple.com/kb/ht4356
- Learn more about iTunes Wi-Fi Sync
  http://support.apple.com/kb/HT1386
- Learn more about iTunes Wi-Fi Sync setup and troubleshooting
  http://support.apple.com/kb/TS4062

Configuration and Management

There are three ways to configure and manage iOS devices: manually on the device, using configuration profiles, and using a Mobile Device Management solution.

Manually Configuring Devices

Restrictions and configuration information can be set directly on each iOS device. This is the simplest configuration method but requires manually configuring each device. This may be optimal for small deployments or in self-service scenarios.

Certain restrictions can only be set directly on the device in the Settings app, including the abilities to delete apps; change accounts for Mail, Contacts, and Calendars; toggle location services; and make changes to Find My Friends.

Changes to restrictions set directly on an iOS device are protected by a four-digit restrictions passcode that is independent of the device lock passcode used to prevent unauthorized access to the device. The restrictions passcode can only be set or changed directly on the device.

Configuration settings and restrictions are backed up, persist through restoring a device from a backup, and can be included in a master backup on a centralized iTunes computer. After deployment, restrictions must be changed manually on each device, or an updated master backup must be restored to all devices.

- Learn more about device restrictions
  http://support.apple.com/kb/HT4213

Understanding Configuration Profiles

Configuration profiles are XML files that contain device passcode policies, restrictions, account and networking settings, Web Clips, and credentials that permit iPhone, iPad, and iPod touch to work with enterprise systems. Configuration profiles can optionally be locked so that an end user can't remove them without restoring the device. Configuration profiles can be distributed via the Internet or email or can be installed over USB using iPhone Configuration Utility.

Configuring Accounts and Credentials Using Configuration Profiles

Configuration profiles can install account and configuration information for use with Exchange ActiveSync, IMAP/POP/SMTP Email, CalDAV calendar services, CardDAV and LDAP address book services, Wi-Fi networks, VPN services, and subscribed calendars. Profiles may include account settings as well as credentials for the account. If a profile does not include credentials, the user is prompted for a password upon manual installation of the profile.

Configuring Restrictions Using Configuration Profiles

Institutions can prevent the downloading and use of unauthorized apps by enabling the Installing Apps restriction. This restriction also prevents syncing or updating apps in iTunes and must be removed to allow installing new or updated apps.

- Learn more about updating apps in the *Planning for App and iOS Updates* section of the *Deployment Strategies* chapter of this document.

Institutions who want to restrict Internet access may choose to enable the Safari restriction, which removes the Safari icon from the Home screen. Several third-party filtered web browser apps are available from the App Store.

- Learn more about configuration profiles
  http://developer.apple.com/library/ios/featuredarticles/iPhoneConfigurationProfileRef

Web Clips

A Web Clip is an icon on the device Home screen that links to a website. Web Clips can optionally launch full-screen web apps and can run offline by leveraging HTML 5 local storage.

Configuration profiles can include Web Clips that use a custom title and icon and can optionally be set to be nonremovable. Consider including a Web Clip in a large deployment to facilitate future management and configuration of devices. You can use Web Clips to easily direct users to future deployment information, such as new configuration profiles, recommended App Store apps, and enrollment in a Mobile Device Management solution.

- Learn more about Web Clips
  www.apple.com/webapps/whatarewebapps.html

Using iPhone Configuration Utility

iPhone Configuration Utility (iPCU) allows institutions to easily create, maintain, encrypt, and install configuration profiles, and in-house apps. You can also use it to capture device information, including console logs.

- Learn how to use iPhone Configuration Utility
  http://developer.apple.com/library/ios/#featuredarticles/FA_iPhone_Configuration_Utility/Introduction/Introduction.html

Using Mobile Device Management Solutions

iOS Mobile Device Management (MDM) capabilities give education institutions the ability to securely enroll devices in an enterprise environment, wirelessly configure and update settings, monitor institution policy compliance, deploy apps, and remotely wipe or lock managed devices. MDM solutions are provided by third parties, offering support for a variety of server platforms, management consoles, additional features, and pricing structures. Evaluate which aspects of MDM solutions are most relevant to your organization before you choose a solution.

- Learn more about Mobile Device Management
  www.apple.com/iphone/business/integration/mdm

Requirements

Mobile Device Management requires that devices be running iOS 4 and later. Some features only work with iOS 5 clients.

Enroll

Enrollment of devices enables cataloging and asset management. The enrollment process leverages SCEP (Simple Certificate Enrollment Protocol) so iOS devices can perform over-the-air enrollment of identity certificates for authentication to institution services. MDM enrollment is both user opt-in and opt-out. Institutions should consider incentives for users to remain managed. For example, you could require MDM enrollment for Wi-Fi network access by using the MDM solution to automatically provide the wireless credentials. With iOS 5, when a user unenrolls from MDM, the device attempts to notify the MDM server.

Configure

Once a device is enrolled, it can be dynamically configured with settings and policies by the Mobile Device Management server. The MDM server accomplishes this by sending configuration profiles to the device that are installed automatically without the user's intervention.

When combined with enrollment, device configuration provides assurance that only trusted users are accessing institution services and that devices comply with established policies. Configuration profiles can be signed, encrypted, and locked, preventing the settings from being altered or shared. This means that if users want to remove management settings, they must opt out of the MDM solution and lose access to the institution's network resources.

Query

A Mobile Device Management server has the ability to query devices for a variety of information. This includes hardware information such as serial number, device UDID, or Wi-Fi MAC address, and software information, such as the iOS version and a detailed list of all apps installed on the device. This information can be used to ensure that users maintain the appropriate set of apps.

Manage

When a device is managed, it can be administered by the Mobile Device Management server through a set of specific actions. Management tasks include changing configuration settings, remotely wiping a device, and clearing a passcode lock.

Managed Apps

With iOS 5, Mobile Device Management servers can deploy both App Store and in-house enterprise apps to devices over the air. Users are prompted to install or update apps that can be removed remotely by the server, along with the data associated with each app. Apps deployed from an MDM server can optionally be prevented from backing up data to iCloud or iTunes and can be removed if the user unenrolls from MDM.

Apple Push Notification Service

All MDM solutions use the Apple Push Notification Service (APNs) to maintain persistent communication with devices across both public and private networks.

- Learn more about APNs
  http://support.apple.com/kb/HT3576
- Learn more about required firewall ports for APNs and other services in the *Understanding Firewall Requirements* section of the *Preparing for Deployment* chapter of this document.

Profile Manager

OS X Lion Server includes Profile Manager, a server-based solution for remotely managing iOS devices and Mac systems running OS X Lion. Profile Manager simplifies creation of configuration profiles, enforcement of restrictions through Mobile Device Management, and deployment of iOS in-house apps.

Profile Manager also gives users access to a self-service web portal where they can download and install new configuration profiles. User can use this web portal to perform tasks such as clearing passcodes and remotely locking or wiping devices that are lost or stolen.

Lion Server is available from the Mac App Store and can be used to transform a Mac running OS X Lion into a Lion Server. It is also available preinstalled on a Mac mini or Mac Pro with Lion Server. There are no client licenses to purchase or maintain to use the features of Lion Server, which makes Profile Manager the simplest and fastest way to get started with Mobile Device Management.

- Learn more about Profile Manager
  www.apple.com/macosx/server
  http://help.apple.com/profilemanager

Using Exchange ActiveSync

iPhone and iPad can communicate directly with Microsoft Exchange Server via Microsoft Exchange ActiveSync (EAS), enabling push email, calendars, contacts, and tasks. Exchange ActiveSync also provides users with access to the Global Address List (GAL) and provides administrators with passcode policy enforcement and remote wipe capabilities. iOS supports both basic and certificate-based authentication for Exchange ActiveSync. If Exchange ActiveSync is already enabled, the necessary services are already in place to support iPhone and iPad with no additional configuration required.

- Learn more about Exchange ActiveSync on iOS
  http://images.apple.com/iphone/business/docs/iOS_EAS.pdf

Purchasing Content

Institutions can choose from a variety of methods for purchasing apps, books, and iBooks textbooks. Education users, like all iTunes users, can use credit cards or gift cards to fund individual purchases. To purchase apps and books in volume, education institutions can use the Volume Purchase Program (VPP) and fund purchases via purchase order, credit card, or PCard. If an institution is tax exempt, it is not charged sales tax when purchasing content through VPP. An institution may choose one or more purchasing methods depending on its needs.

- Learn about great learning apps
  www.apple.com/education/apps

Purchasing with a Credit Card or iTunes Gift Card

Anyone in the U.S. aged 13 years or older can purchase apps, books, and iBooks textbooks from the iTunes Store with a credit card or an iTunes Gift Card. iTunes Gift Cards are readily available in many retail locations throughout the United States as well as directly from Apple Education Sales. Credit cards and iTunes Gift Cards share a similar set of advantages and requirements.

Apps and books are purchased one at a time with either of these funding sources, and each can only be purchased once per iTunes account. The entire balance of a gift card must be used by one iTunes account and can't be shared with other iTunes accounts. Therefore, neither of these purchasing methods is appropriate for volume purchasing.

Additionally, tax-free purchasing is not possible with iTunes Gift Cards or credit cards. Consider the Volume Purchase Program if frequent tax-free app purchasing is required.

Examples of purchases funded by credit card may include school administrators using institutional PCards to purchase apps or books for individual use, instructors purchasing apps or books for use only on their devices, or college students using personal credit cards to purchase apps or books that may be required for a particular course. Some institutions may choose to provide gift cards to instructors to allow them to experiment with new apps in the App Store before deciding to purchase in volume using the Volume Purchase Program.

Volume Purchase Program

The Volume Purchase Program allows educational institutions to purchase iOS apps and books in volume and distribute them to students, teachers, administrators, and employees (terms and conditions apply). The program also allows app developers to offer special pricing for purchases of 20 apps or more. K–12 and degree granting higher education education institutions in the United States qualify for participation in the Volume Purchase Program.

VPP Workflow

There are three roles involved in the VPP process: the Program Manager, the Program Facilitator, and the End User. These three roles allow for multiple purchasing and deployment workflows depending on the needs of the education institution.

Understanding Program Roles

Program Manager

A Program Manager for VPP is responsible for enrolling an institution in VPP. A Program Manager for VPP is also authorized by the educational institution to create and manage Program Facilitator accounts.

Program Facilitator

Program Facilitators can redeem Volume Vouchers through the VPP portal. They can search for and order apps and books in variable quantities, spending up to the current dollar amount credited to their account via redeemed Volume Vouchers. Program Facilitators can also purchase apps and books at the Volume Purchase Program store using credit cards, PCards, and PayPal.

Program Facilitators can be anyone designated by the Program Manager—for example, deans, professors, researchers, principals, teachers, technology coordinators, or instructional technologists. This role may correlate to the person already responsible for procuring software for your institution. The person serving as the Program Manager can also act in this role, although a separate Program Facilitator account is required.

The Program Manager creates a new Apple ID for each Program Facilitator to use exclusively within the VPP store. Existing Apple IDs can't be used within VPP. A valid email address that is not currently used as an Apple ID needs to be provided to Apple for each Program Facilitator. This email address should be controlled by your education institution to ensure that the Volume Vouchers redeemed with the Program Facilitator account aren't tied to an individual.

End User

For the purposes of VPP, the End User is any iTunes account used to redeem apps and books.

For app purchases, education institutions have the option of redeeming one app code per iTunes authorized computer, or "sync station," and retaining the rest of the codes as proof of purchase. Therefore, the End User iTunes account may also be created using a school-controlled email address, and the sync station administrator should be an authorized user.

For book purchases, an institution may not use a single code to sync an iBookstore product to multiple devices. The iBookstore product may not be used in a library-type lending scenario.

iTunes accounts can be created without a credit card, which may be useful for creating institution iTunes accounts.

- Learn more about iTunes accounts in the *Understanding iTunes* section of the *Deployment Strategies* chapter of this document.

Enrolling in the Volume Purchase Program

Education institutions that qualify for enrollment in VPP can sign up for the program online.

- Learn more about enrolling in VPP
  www.apple.com/education/volume-purchase-program
- Read frequently asked questions about VPP
  www.apple.com/education/volume-purchase-program/faq.html

Understanding Volume Vouchers

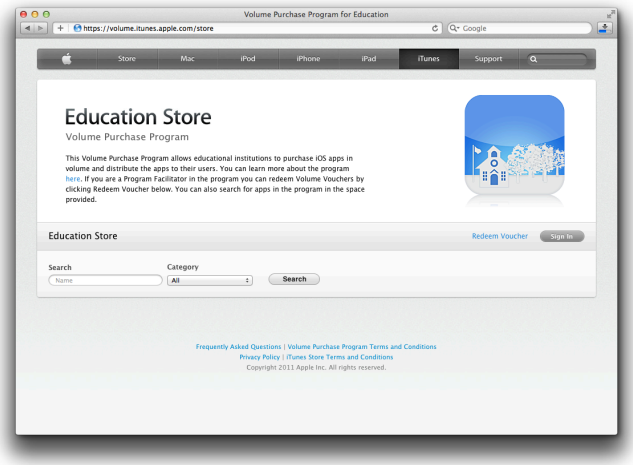
Volume Vouchers are physical cards in denominations of $100, $500, $1000, $5000, and $10,000 that can be used only to purchase apps within the VPP store. They are shipped via Federal Express or UPS, so they can be easily tracked and should arrive within three to five business days from the time of the order.

Volume Vouchers can only be used in the VPP store and are not valid for regular iTunes, App Store, or iBookstore downloads. This means that lost or stolen Volume Vouchers cannot be redeemed by anyone who is not a registered user of VPP. Each Volume Voucher can be used by one Program Facilitator account. Purchase multiple vouchers in smaller denominations if funds need to be distributed to multiple Program Facilitators.

Using the Volume Purchase Program

Only Program Facilitators purchase apps and books through the VPP Education Store, but anyone can browse the store. This makes it easy for anyone to check pricing at any time, even if that person isn't designated as a Program Facilitator.

When purchasing, the Program Facilitator must enter a value in the quantity field. Institutions that are eligible for tax-free purchasing aren't charged tax when purchasing via the VPP Education Store or when purchasing Volume Vouchers. Following each purchase, the Program Facilitator receives a spreadsheet that includes a list of redemption codes that can be redeemed by End Users in iTunes. The Program Facilitator can download updated versions of the spreadsheet to review which codes have been redeemed.



- Browse the VPP store
  http://volume.itunes.apple.com

Volume Pricing

Many app developers offer volume pricing on their titles through VPP. If the developer has enabled volume pricing, purchasers receive 50% off when purchasing 20 or more licenses of an app. The volume pricing is applied per purchase, meaning that previous and future app purchases aren't taken into account.

Reminder*:* If possible, coordinate and consolidate app purchase requests to reach the volume pricing at 20 or more licenses of an app.

Volume pricing is not available for books or iBooks textbooks.

Code Distribution Techniques

Distribution of redemption codes is the responsibility of the educational institution. Codes can be distributed manually to users, emailed via a mail merge process, or posted to an internal website such as a wiki. Organizations can create their own code distribution website to distribute codes to users. Some Mobile Device Management solutions integrate VPP code redemption into their self-service client applications.

The spreadsheet of codes obtained from VPP includes a URL for each unique code. Each URL includes the associated code and can serve as a shortcut for distributing app redemption codes to users. The URL structure is as follows:

https://buy.itunes.apple.com/WebObjects/MZFinance.woa/wa/freeProductCodeWizard?code=REDEMPTIONCODEHERE

Replace *REDEMPTIONCODEHERE* with the actual redemption code for the app.

These URLs can be used to obscure the code from the user when building a code distribution website or service to create a more seamless integration process.

- Read VPP frequently asked questions for examples
  www.apple.com/itunes/education/faq

Deployment Strategies

A critical question that influences all aspects of a deployment is: Who owns the apps? The answer is either the individual end user or the institution, which means that either the user's iTunes account is used to redeem a VPP app code or the institution's iTunes account redeems it. Whichever iTunes account is used retains ownership of the app license. This chapter discusses deployment models for end user ownership (Personal Ownership model), institutional ownership (Institutional Ownership model), and a hybrid of both (Layered Ownership model).

Each of these deployment models has unique implementation details that should be fully understood before deployment.

- For more information about how Apple can assist with iOS deployment design and execution, see the Apple Professional Services section of the Preparing for Deployment chapter of this document.

Common to all three models is the use of iTunes.

Understanding iTunes

Apple IDs

An Apple ID is the login used for just about everything Apple offers, including using iCloud to store content, downloading apps from the App Store, and buying songs, movies, and TV shows from the iTunes Store.

Each Apple ID must be created using a unique email address. Account design varies depending on the deployment strategy, and institutions may prefer iTunes Store accounts to be created without a credit card.

The email address used to create an iTunes Store account is the Apple ID, which allows access to all other Apple services. It isn't necessary to create a new account for each service—just use the same Apple ID.

- Learn more about Apple ID
  www.apple.com/support/appleid
- Learn more about creating iTunes accounts without a credit card
  http://support.apple.com/kb/HT2534
- Learn more about associating devices and computers to an Apple ID
  http://support.apple.com/kb/HT4627

iTunes in the Cloud

The services included with iCloud, including iTunes in the Cloud, are for personal use only and should not be used by institutions.

- Learn more about iTunes in the Cloud
  www.apple.com/icloud/features

Deploying iTunes

iTunes on the Mac or PC stores all content in the iTunes library, which resides in the user's home folder. When an iOS device is synced with iTunes, it becomes paired to the iTunes library on that particular computer. This means that the iOS device can't sync with another computer without first erasing the existing apps or content.

- Learn more about iTunes libraries
  http://support.apple.com/kb/ht1660

Home Sharing can be used to transfer purchased content, including apps, between computers authorized to use the same iTunes account without downloading the content again from the iTunes Store.

- Learn more about the Home Sharing feature in iTunes
  http://support.apple.com/kb/ht3819

Each iTunes account can be authorized for use on up to five computers, and each computer can sync an unlimited number of iOS devices. To deauthorize a computer, choose Deauthorize Computer from the Store menu in iTunes on that computer.

To simultaneously deauthorize all computers currently associated with an iTunes account, click the Deauthorize All button in the Account Information pane in iTunes. The Deauthorize All button does not appear if there are fewer than five authorized computers for the iTunes account or if this option has been used within the last 12 months. You should carefully plan the authorizing and deauthorizing of computers to reduce the need to use the Deauthorize All feature in iTunes.

- Learn more about iTunes Store authorization and deauthorization
  http://support.apple.com/kb/ht1420

iTunes account passwords should be closely guarded to prevent unauthorized use.

- Learn more about protecting iTunes accounts
  http://support.apple.com/kb/HT4156

iTunes is used to name connected iOS devices. Uniquely naming devices can make network identification and ongoing maintenance easier.

- Learn more about renaming devices in iTunes
  http://support.apple.com/kb/ht3965

iTunes is used to back up, restore, and upgrade iOS devices. Devices can only sync with one computer, so plan where devices will be synced before restoring them from a backup. Be sure to back up devices and sync any media content prior to upgrading.

- Learn more about upgrading to iOS 5
  http://support.apple.com/kb/HT4972
- Learn more about how to back up devices
  http://support.apple.com/kb/HT4079
- Learn more about using iTunes
  www.apple.com/support/itunes

Managing Documents

Depending on the capabilities of the app in use, there are many ways to get content in or out of an app. Some common methods for distributing content include wikis or other websites where users can open a posted file directly in an installed app. Some common methods for exporting content from an app include email or a WebDAV file server.

Deployment Models

Strategies for the initial setup and ongoing maintenance of devices are based on app ownership—whose iTunes account will be used to redeem the app codes your institution purchases in volume.

If only the end user will own the apps, the Personal Ownership model is ideal. If only the institution will own the apps, the Institutional Ownership model is the best fit. However, if devices will have content owned by the institution as well as content owned by the end user, the Layered Ownership model is preferred.

Personal Ownership Model

The Personal Ownership model is similar to the typical consumer experience. The education institution may or may not own the iOS device, but the end user takes responsibility for ongoing maintenance and retains ownership of all apps and content. A personal ownership strategy has the least impact on support resources because many care and maintenance responsibilities are shifted to the end user. The deployment timeline can be accelerated because little preparation work on devices is required. Users may also be more protective of assigned devices if they can personalize content.

The Personal Ownership model delivers the optimal user experience for students who are at least 13 years old and allowed to customize their own devices.

Some educational institutions may prefer that the end users, whether they are administrators, instructors, or students, own their devices or content or both, making a Personal Ownership strategy attractive. If an educational institution provides VPP app redemption codes in this model, the end user's personal iTunes account retains ownership of the app license.

Configuration and management tools can be used as part of the deployment to allow the institution to control the settings and configuration of the devices. iPhone Configuration Utility can be used to install configurations and set restrictions. A Mobile Device Management solution may be employed for centralized wireless configuration and management as well as for portal-based VPP app redemption code distribution.

- Learn more about Mobile Device Management in the *Configuration and Management* chapter of this document.

Implementing a Personal Ownership model is a straightforward process. Regardless of who owns the device, the end user either syncs with iTunes using a personal Apple ID or chooses to be PC-free by using a personal Apple ID for iCloud services.

The general workflow for implementing the Personal Ownership model is:

1. Asset tag or inventory devices as needed.
2. Deploy to end users.
3. Each end user completes iOS 5 Setup Assistant using his or her personal Apple ID.
   - iCloud services are enabled.
   - iCloud backup is enabled.
4. The end user enrolls in MDM (if it is being used).
5. Deliver app redemption codes to end users, which they redeem using a personal iTunes account.

Institutional Ownership Model

Because the Personal Ownership model requires that app licenses are owned by the personal Apple ID of the end user, some institutions may want to use the Institutional Ownership model instead. Syncing multiple devices to a centrally controlled iTunes account gives education institutions a way to retain ownership of all app purchases.

Rather than the end user managing VPP app redemption codes, the institution performs all app code redemptions on sync stations, which are computers running iTunes using an Apple ID that the institution owns and controls. To receive new or updated apps that the institution has purchased, each iOS device must continue to be synced with the iTunes library from which it was first configured.

The Institutional Ownership model is preferred for temporary device usage and for deployments in which end users are under 13 years old.

If an attempt is made to sync a device to another computer, iTunes notifies the user that the apps and content synced by the institution's sync station must be erased from the device before the new computer can sync to it. A student missing all of the institution's curriculum apps will quickly stand out when he or she is unable to participate in class projects requiring those apps.

For the best performance and reliability, the latest versions of iTunes and OS X should be used when syncing multiple devices simultaneously. iTunes for Windows works best with only one device connected at a time.

- Learn more about connecting multiple devices to iTunes for Windows http://support.apple.com/kb/HT3622

Device restrictions can be enabled to prevent users from installing or deleting apps or making other changes to the device configuration. Some restrictions can only be set manually on each device. Other restrictions and settings can be applied using iPhone Configuration Utility or managed wirelessly via a Mobile Device Management solution.

- For more information about configuring and managing iOS devices, see the *Configuration and Management* chapter of this document.

Implementing the Institutional Ownership Model

Implementing an Institutional Ownership model requires that iTunes accounts be created using email addresses under the control of the education institution. Sync stations are strategically placed within the building or on carts and are authorized to use an iTunes account that is not tied to a credit card.

The following is the workflow for an institution to implement the Institutional Ownership model:

1. Starting with a new or factory-defaults device running iOS 5, sync the required institution apps to the device. Complete iOS 5 Setup Assistant (this must be completed by the institution).

   Note: Skip the Apple ID prompt because iTunes manages this.

2. Customize settings and restrictions on the device.
3. Place icons in folders (if desired).
4. Enroll the device in MDM (if it is being used).
5. Disable the App Store.
6. Deploy devices to users.

7. App redemption codes are redeemed by the institution's Apple ID on the iTunes sync station only.

   Note: Because it is important to prevent personalization of devices with the Institutional Ownership model, the App Store should be disabled on the devices.

8. Learn more about creating iTunes accounts without a credit card in the *Understanding iTunes* section of this chapter.
9. Learn more about iTunes account strategies in the *Understanding Sync Stations* section of this chapter.

Configuring iTunes

Configure iTunes for optimal syncing with multiple devices before first use. In the General pane of iTunes preferences, deselect (if selected) the "Check for new software updates automatically" option. This prevents the display of software update messages as each device is connected.

If end user data from iOS devices does not need to be regularly backed up by the sync station, you may turn off automatic backups.

To disable automatic backups, type the following in Terminal:

```
defaults write com.apple.iTunes
AutomaticDeviceBackupsDisabled -bool true
```

Devices will be allowed to sync but automatic backups won't be performed. While automatic backups are disabled, all device backups must be performed manually.

To turn on automatic backups, type the following in Terminal:

```
defaults write com.apple.iTunes
AutomaticDeviceBackupsDisabled -bool false
```

After the iTunes sync stations have been configured, apps can be downloaded from the iTunes Store. Your institution must already be enrolled in the Volume Purchase Program to sync apps to multiple institution-owned devices using one iTunes account.

- Learn more about purchasing and redeeming apps in the *Purchasing Apps* chapter of this document.

After all required apps have been redeemed and downloaded on the iTunes sync station, one or more master backups can be created. A master backup acts as a template. To create a master backup, you configure one iOS device exactly the way you want all devices to be configured, and then you create a backup of that device with iTunes. Consult with the appropriate stakeholders to ensure a master backup meets curriculum and IT requirements. Complete iOS 5 Setup Assistant on the master device and skip signing in with an Apple ID. The Apple ID of the sync station is used exclusively because no end user personal content will be allowed.

- Learn more about backing up and restoring devices with iTunes in the *Understanding iTunes* section of this chapter.

Consider setting the restrictions passcode on the master device to prevent students from setting the code later or enabling device restrictions. Setting the Restrictions passcode, preventing deletion of apps, disabling location services, and preventing modification of email accounts can only be done directly on the device, so these settings may be part of the master backup.

- Learn more about restrictions in the *Configuration and Management* chapter of this document.

After you make a master backup with iTunes, you can connect additional devices to the iTunes library and restore them from the original backup. When you connect new iOS devices or ones that haven't been configured to the computer, iTunes displays a prompt to restore the device from a backup.

- Learn how to build a master backup in the *Preparing a Sync Station* section of this chapter.

Once the iOS device used to create the master backup is renamed, iTunes renames and replaces the original backup with personalized data from the new end user of the device. Therefore, the master backup may need to be recreated if there is reason to restore all devices synced to that iTunes library.

Alternatively, you can make a copy of the master backup for easy reuse. iTunes device backups are stored in *~/Library/Application Support/MobileDevice/Backup* and can be copied to other locations. Making a copy of the master backup may make it easier to reuse that backup in the future. Consider designating a folder on the computer or an external volume to store copies of master backups. If any of these backups are needed, simply copy them back to the folder path listed above and overwrite the existing backup. This step destroys the personalized backup data for the device used to create the master backup being copied.

Management and configuration tools can be used after each device has been restored from the master template. You can use iPhone Configuration Utility to install configuration settings and restrictions or you can use a Mobile Device Management solution for centralized wireless configuration and management.

If you want to restrict end users from installing additional apps on their iOS devices, consider setting the App Installation restriction. This restriction prevents all app installations, including using iTunes on the institution sync station. A Mobile Device Management solution can facilitate the process of changing the App Installation restriction on multiple devices at once.

- Learn more about restrictions in the *Configuration and Management* chapter of this document.

Understanding USB

A wide variety of USB based peripheral devices are available and many have unique power requirements. The USB ports on Apple computers and displays provide 500 mA (Milliamps) at 5 V (Volts) to each port, regardless of whether the port is USB 1.1 or USB 2.0. This is in compliance with USB specifications.

Some Apple peripheral devices, including iPhone, iPad, and iPod touch, may request more than 500 mA (Milliamps) at 5 V (Volts) from a port to function or to allow for faster charging.

- Learn more about powering USB peripherals
  http://support.apple.com/kb/HT4049

The experience of syncing and charging multiple devices can vary depending on the selection of a USB hub. For best results consider products that have the Made for iPhone, Made for iPad, or Made for iPod logo.

These logos mean that the accessory has been designed to connect specifically to iPhone, iPad, or iPod touch and has been certified to meet Apple performance standards. Apple iPad Learning Labs and Apple iPod Learning Labs meet these requirements.

- Learn more about Apple mobile learning labs www.apple.com/education/labs
- Learn more about the Made for iPhone, Made for iPad, and Made for iPod logos http://support.apple.com/kb/ht1665

Understanding Sync Stations

Sync station computers may be deployed as stationary systems or as part of a mobile cart. MacBook, MacBook Pro, or MacBook Air work best with carts because they can run on battery power and are easily stored inside the cart. Desktop computers must be powered off before transporting the cart and may pose a safety hazard while the cart is being moved.

Determining where devices will be used affects how your institution's iTunes accounts are provisioned. In turn, the iTunes account design determines sync station placement. Sync station designs vary depending on the deployment goals, and more than one sync station design strategy may exist in the same building.

iTunes accounts can be created based on logical groupings within the organization. For example, sharing a generic iTunes account within a department or grade level may facilitate collaboration between instructors in selecting the most effective apps. The examples below describe some possible iTunes account designs, but other configurations may be used, depending on your institution's needs.

Preparing a Sync Station

Plan for scalability when designing and configuring sync stations. It's easier to deploy the first few sync stations if you already know the long-term goals.

Before preparing a sync station, be sure to:

- Learn more about iTunes accounts in the *Understanding iTunes* section of this chapter.
- Learn more about restrictions and configuration profiles in the *Configuration and Management* chapter of this document.

The steps below require a Mac connected to the school network running the latest version of OS X, iTunes, and iPhone Configuration Utility. The email address for the iTunes account should already have been created, but not the iTunes account itself.

1. Create a new OS X account for the sync station end user.
   a. Consider setting the Full Name to something easily readable by the end user (for example: 1st Grade Sync).
   b. Consider setting the Short Name to match the user name of the iTunes account email address (for example: school.itunes.1st).
2. Log in to the Mac using the OS X account created in the previous step.
3. Configure iTunes.
   a. Launch iTunes and create a new iTunes account without a credit card using the email address created for it.

b. Authorize iTunes to use this iTunes account by choosing Authorize This Computer from the Store menu.

c. Redeem apps purchased through VPP and download required free apps.

d. Add other media to the iTunes library such as audio, video, ePub documents, PDFs, or podcasts (if applicable).

Reminder: Verify volume licensing before syncing apps to devices.

4. Build an iOS device master backup.

a. Designate a device to build the master backup.

b. Activate and name the device with iTunes (for example: 1st Grade Master iPad).

c. Sync the device with iTunes to load desired content.

d. Configure device settings and restrictions, such as:

- App folders and Home screen icon layout (on device or in iTunes)
- Restrictions passcode (recommended)
- Deleting the Apps restriction (if applicable)
- Location restriction (if applicable)
- Accounts restriction (if applicable)

e. Sync and then back up the device with iTunes.

The sync station has been configured and can now be deployed. The remainder of the devices for this cart can be restored from the master backup upon connection to iTunes. After a device is restored from the backup, it can be renamed in iTunes and configuration profiles can be installed.

Preparing Multiple Sync Stations

If several sync stations will use the same iTunes account, perform the additional steps below. The additional sync stations must meet the same requirements as the initial sync station.

These instructions make use of Migration Assistant to create additional sync stations and have the same requirements as the Preparing a Sync Station procedure above.

Learn more about Migration Assistant
http://support.apple.com/kb/HT4413

On the initial sync station:

1. Enable Home Sharing in iTunes.
2. Launch Migration Assistant.
   - Select "To another Mac" as the migration method and then click Continue. The initial sync station is now ready to copy the OS X user account that contains the iTunes library content and device backups to the next sync station.

On the additional sync station:

1. Launch Migration Assistant.

a. Select "From another Mac" and then select Use Network if prompted.

b. On the *initial* sync station, enter the code that appears on the additional sync station and then click Continue.

c. Click Continue and ensure only the OS X user account created for the sync station end user is selected. The process begins.

2. Log in to the copied OS X user account.
   a. Launch iTunes and authorize the computer to use the same iTunes account as the initial sync station.
   b. Verify that iTunes contains the same content and backups as the initial sync station.

   Repeat the process above to add sync stations using the same iTunes account. Immediately after you have completed these steps, all sync stations will have identical apps and content to sync with iOS devices. Afterwards, the sync stations can update apps and content independently of each other. You can use Home Sharing in iTunes to easily copy new and updated apps between sync stations.

   Reminder: Verify volume licensing before syncing apps to devices.

   - Learn more about Home Sharing in iTunes http://support.apple.com/kb/ht3819
   - Learn more about volume licensing for syncing apps to multiple devices in the *Purchasing Apps* chapter of this document.

   Repeat the steps in "Preparing a Sync Station" and "Preparing Multiple Sync Stations" for additional sync stations that share a different iTunes account.

Planning for App and iOS Updates

Because syncing, updating apps, and applying iOS updates for a large number of devices may become time consuming, consider establishing a sync and upgrade schedule. For example, you could schedule app or iOS updates quarterly, biannually, or during winter, spring, and summer breaks.

Test existing apps on new versions of iOS before upgrading all devices because some apps may need to be updated before they'll work with a new iOS version. A similar plan may be considered for app updates so that all students and instructors use the same version of any particular app. Don't postpone iOS upgrades indefinitely because some app updates may require a newer iOS version.

Designing iTunes Accounts for Grade Level Use

In an elementary school setting where students will store devices in a classroom cart, consider assigning one iTunes account per grade level. A sixth sync station in a grade level will require a new iTunes account because the previous account will have reached the five authorization limit. This means that if a school has six to ten classrooms in one grade level, it may be optimal to use one iTunes account for half of the sync stations and a second account for the other half to allow collaboration for instructors sharing each iTunes account.

Additionally, consider naming the email addresses that will be used to create iTunes accounts accordingly. For example, the email address you use to create the kindergarten iTunes account could be in the format of *school.itunes.k@xx.k12.xx.us*, the address you use to create the first grade iTunes account could be in the format of *school.itunes.1st@xx.k12.xx.us*, and so on, where *school* is replaced with the actual name or abbreviation of the school. Including the school name within the email address is helpful in large deployments where multiple schools cover the same grade levels. These email addresses are just examples, so you may use an alternate naming scheme.

Designing iTunes Accounts for Department Use

Similar design considerations apply to middle or high schools and higher education. However, in this environment the iTunes accounts would be built around the content areas or academic disciplines instead of grade levels. In a content area scenario, the email addresses you use to create iTunes accounts may be in the format of *building.itunes.math@institution.edu*, where *building* is replaced with the actual name or abbreviation of the building. If more than five sync stations are needed in any given department, you could add a number to the email address for the second account: *building.itunes.math2@institution.edu*. Including the building name within the email address is helpful in large deployments where multiple buildings cover the same content areas. These email addresses are examples; you may use an alternate naming scheme.

Designing iTunes Accounts for School and Home Use

When centrally synced devices are assigned to students to take home, they must be assigned to a sync station. In this scenario, the iTunes account design is more generic than with the grade level or department designs. Students could be assigned to a sync station in a particular room, based on grade level or other criteria the institution prefers.

The email address used to create the iTunes account for the building could be in the format of *school.itunes@xx.k12.xx.us*, where *school* is replaced with the actual name or abbreviation of the school. This iTunes account can then be authorized on a total of five sync stations to minimize the number of iTunes accounts per building. This email address is an example, so you may use an alternate naming scheme.

For example, if you're assigning students to sync stations in a specific room, consider provisioning a total of five sync stations authorized with the same iTunes account. Sync stations might be placed in the library or other rooms with student access. Once students are assigned to a sync station, they must continue to use that sync station to get new apps or updates, or the devices may be erased to sync with a new sync station and get different apps.

If more sync stations are needed, this design could be expanded by using more than one iTunes account.

Modifying iTunes Accounts

iTunes account information such as name, password, email address, payment method, and billing address can be updated using iTunes.

- Learn more about updating iTunes account information
  http://support.apple.com/kb/HT1918

Managing Apps and Content

In the examples above, the sync station design matches the logical grouping of instructors. Additionally, if instructors participate in professional learning communities, they probably meet regularly to discuss student data. As discussions turn to what apps are most effective for a particular content area, instructors may benefit from quick access to the most appropriate apps.

The Home Sharing feature in iTunes can facilitate sharing of apps and content between sync stations that use the same iTunes account.

Reminder: Verify volume licensing before syncing apps to devices.

- Learn more about Home Sharing in the *Understanding iTunes* section of this chapter.
- Learn more about volume licensing for syncing apps to multiple devices in the *Purchasing Apps* chapter of this document.

Layered Ownership Model

While a Personal Ownership deployment allows the individual to own all content and an Institutional Ownership deployment allows the institution to retain ownership of all content, the Layered Ownership deployment allows for both parties to own their respective content on the same device.

The Layered Ownership model offers the end user full control over his or her content while allowing the institution to retain ownership of purchased apps. This makes it an excellent deployment strategy for all users age 13 and over.

Syncing with an institution's iTunes account allows an organization to ensure that a prescribed set of apps exists on all iOS devices. These apps are synced to a device that has not yet completed iOS 5 Setup Assistant. Typically, the device is new or at factory defaults and must be running iOS 5.0 or later.

The end user then uses his or her personal Apple ID to complete iOS 5 Setup Assistant, which configures built-in apps and services to use the personal Apple ID, including a personal iTunes account. The institution continues to manage apps from iTunes while the end user manages personal apps and content directly on the device. In the Layered Ownership model, the end user does not sync with any iTunes computer other than the institution's sync station.

Allowing end users to download personal apps and content is more likely to give them a sense of ownership so they may be more apt to protect the iOS devices. This may be helpful in a model where the devices are taken home, and the goal is to both guide and empower the end users. It may also be preferred for iOS devices provided to instructors and administrators.

Implementing the Layered Ownership Model

The implementation of the Layered Ownership model starts with the same basic requirements of the Institutional Ownership model followed by the requirements of the Personal Ownership model. The freedom to personalize the device is preserved from the Personal Ownership model while the ability to retain ownership of apps is preserved from the Institutional Ownership model.

Although the App Store is generally disabled in the Institutional Ownership model to prevent personalization, it must be enabled for the Layered Ownership model.

All new or factory default iOS 5 devices start with a screen prompting the user to "slide to set up." This is the start of iOS 5 Setup Assistant. The end user must complete iOS 5 Setup Assistant to automatically personalize their assigned device with his or her personal Apple ID.

The general workflow for implementing the Layered Ownership model is:

1. Starting with a new device running iOS 5, sync the required institution apps to the device. iOS 5 Setup Assistant must not be completed by the institution.

2. After institution apps are installed, the device is delivered to the assigned user.
3. The end user completes iOS 5 Setup Assistant using his or her personal Apple ID.
   a. iCloud services are enabled.
   b. iCloud backup is enabled.
4. The end user enrolls in MDM (if it is being used).
5. App redemption codes for apps purchased by the institution are redeemed on iTunes sync stations.
6. The end user downloads personal apps directly on the device using his or her personal Apple ID.

   All app data is backed up by the sync station regardless of which account was used to purchase the apps. If an iOS device is restored from a backup using iTunes on the institution's sync station, the user data from the personally owned apps is restored as well and is automatically available once the apps are downloaded again directly on the device using the personal account. Until the personally purchased apps are downloaded again to the device, the data from those apps can be overwritten if available storage on the device becomes low.

   Consider utilizing iCloud Backup instead of iTunes to back up devices if end users have Internet access at home. When iCloud Backup is enabled, the iOS device automatically backs up all user data and settings over the Internet to the end user's personal iCloud storage. This can greatly simplify workflows for the institution as the sync station is only used for syncing new and updated apps. Additionally, eliminating backups at the sync station speeds up the syncing process because one less step must be completed.

   Finally, when syncing to the institution's iTunes account and then using a personal iCloud account directly on the device, the only way to sync to iTunes on a different computer is to erase the apps and content synced by the institution's sync station. Users shouldn't sync with iTunes on their personal computers if the device is already syncing to an institution sync station.

   - Learn about using multiple computers to manage music
     http://support.apple.com/kb/HT1202

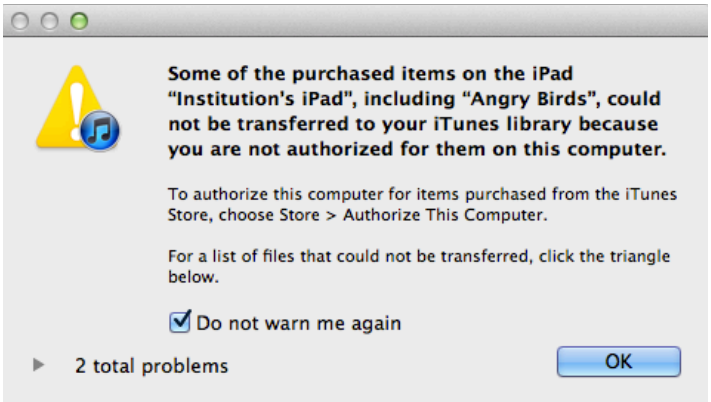
About the Layered Ownership Model

There are a few caveats to note when implementing the Layered Ownership model.

Once the end user has downloaded apps on his or her personal account, the device has apps that belong to two separate accounts. When updates for any of the institution's apps become available, connect the iOS device to the institution's sync station to sync the updated apps.

The first time the device is connected to the sync station after an end user has added personal apps, iTunes displays additional dialogs during the sync process. iTunes alerts the user that apps that aren't authorized for that sync station can't be transferred to it and user interaction is required to continue the sync process. The user clicks Don't Authorize to continue. No data is deleted from the device.

Selecting the "Do not warn me again" checkbox in the iTunes prompt eliminates these alerts. The end user can then update all remaining apps belonging to his or her personal iTunes account by using the App Store on the iOS device. These iTunes messages appear once per device and do not reappear after the "Do not warn me again" checkbox is checked.



If the end user attempts to update all apps on the device by using the App Store, this may include apps belonging to the institution, in which case the user is prompted for the institution's iTunes account password. Because users shouldn't know this password, institution apps can't be updated directly on the device.

However, if end users repeatedly attempt to enter the institution's iTunes account password with an incorrect password, they may cause the account to be disabled from excessive failed login attempts. Reactivating the account requires action from someone with access to the email address associated with the institution's iTunes account. Educate end users on the app update workflow in this model to reduce the likelihood of this scenario.

- Learn more about activating disabled iTunes accounts
  http://support.apple.com/kb/TS2446

Choosing a Deployment Strategy

Develop your deployment strategy before the rollout begins. The questions below form a basic decision tree to assist in selecting a deployment strategy. Select the model or models that meet the most requirements and keep in mind that multiple strategies may be used across an organization.

App Ownership: Whose apps will be allowed on the device?

- End user only: Consider Personal Ownership.
- Institution only: Consider Institutional Ownership.
- Both: Consider Layered Ownership.

Device Personalization: Are users allowed to personalize settings and content on their devices?

- Yes: Consider Personal Ownership or Layered Ownership.
- No: Consider Institutional Ownership.

Device Update Frequency: How often should apps be updated on the devices?

- Frequently: Consider Personal Ownership or Layered Ownership.
- Infrequently: Consider Institutional Ownership or Layered Ownership.

iCloud: Will iCloud services be used on the device?

- Yes: Consider Personal Ownership or Layered Ownership so that only a personal Apple ID uses iCloud services.
- No: Consider Institutional Ownership.

Other Options

Additional Apple products and services, such as iCloud services and Apple TV, can add value to your iOS device deployment.

Understanding iOS 5 Support for iCloud

iCloud is a service that stores a user's content—mail, contacts, calendars, reminders, bookmarks, notes, photos, and documents—and wirelessly pushes it to associated devices and computers, automatically keeping everything up to date.

iCloud features include:

- Automatic Downloads—New music, app, and book purchases are automatically downloaded to the user's devices.
- Download Previous Purchases—A user can view previous iTunes Store and App Store purchases and download them again if needed.
- Photo Stream—When a user takes a photo on one device, the user automatically gets it on his or her other devices.
- Documents & Data—Documents and data for apps that work with iCloud are stored.
- Find My iPad—A user can locate his or her iPad on a map, display a message, play a sound, lock the screen, or remotely wipe the data.
- A user's iPad can also be backed up to iCloud.

Reminder: iCloud services are for personal use only and should not be used by institutions. This means the institution shouldn't own or control the Apple ID used for iCloud services. For example, an end user would be responsible for using Find My iPad to locate a missing iPad using his or her personal Apple ID. This is the same workflow that has been used for many years for lost textbooks.

An iCloud account includes a free mail account and 5GB of storage for mail, documents, and backup. Purchased music, apps, TV shows, and books, as well as photos in Photo Stream, don't count against free space. An iCloud account requires an Apple ID.

Note: iCloud is not available in all areas, and iCloud features may vary by area.

- Learn more about iCloud
  www.apple.com/icloud

iCloud and other services are all automatically configured to use the Apple ID entered in iOS 5 Setup Assistant. Some services can be disabled through the use of restrictions either entered manually on the device or set via configuration profiles.

Reminder: If the user is under 13 (determined by birthday), an Apple ID is not created, and the user won't be able to configure any iCloud services.

- Learn more about configuration and management in the *Configuration and Management* chapter of this document.

Apple TV

Instructors will find immediate use for Apple TV in their classrooms. Instead of being tethered to the projector cable, instructors are able to walk around the classroom with their iPad by using AirPlay Mirroring through an Apple TV connected to a TV or projector.

Consider testing Apple TV in a controlled environment to ensure the LAN and Wi-Fi networks are properly configured for features like AirPlay Mirroring.

- Learn more about Apple TV
  www.apple.com/appletv
- Learn more about designing Wi-Fi networks for Apple TV in the *Supporting AirPlay, AirPrint, and iTunes Wi-Fi Sync* section of the *Wi-Fi Network Design* chapter of this document.

Troubleshooting Resources

- Learn about troubleshooting steps for iPhone
  www.apple.com/support/iphone
- Learn about troubleshooting steps for iPad
  www.apple.com/support/ipad
- Learn about troubleshooting steps for iPod touch
  www.apple.com/support/ipodtouch
- Learn about troubleshooting steps for Apple TV
  www.apple.com/support/appletv
- Learn about troubleshooting steps for iTunes
  www.apple.com/support/itunes

Summary

This document covers many topics related to iOS deployment in education but certainly not all. The following is a summary of key takeaways from each chapter.

Preparing for Deployment

Plan ahead for an iOS deployment. This includes researching apps, preparing a secure staging area for rollouts, firewall considerations, understanding AppleCare support plans, Apple Professional Services, available Apple factory services, and Apple Professional Development.

Wi-Fi Network Design

Designing Wi-Fi networks requires planning for coverage as well as density of devices within that coverage area. Consideration must also be given to security, Wi-Fi standards, and use of Apple iPad Learning Labs. Consult with a Wi-Fi network provider to determine an optimal design of a Wi-Fi infrastructure to support iOS devices.

Purchasing Apps

Enroll in the Volume Purchase Program before devices arrive to begin researching and budgeting for apps that will be part of the deployment. Identify who will fill the Program Manager, Program Facilitator, and End User roles.

Configuration and Management

There are three ways to configure and manage iOS devices: manually configuring devices, deploying configuration profiles using iPhone Configuration Utility (iPCU), and using a Mobile Device Management (MDM) solution. Understand how each configuration and management option can be used prior to deployment.

Deployment Strategies

There is no one-size-fits-all approach for syncing. Determining who will own purchased apps and content will shape the deployment strategy. The three models are: Personal Ownership model, Institutional Ownership model, and Layered Ownership model.

Appendix A—Wi-Fi Standards

This appendix discusses the Wi-Fi standards related to designing a Wi-Fi network that will include iOS devices. The selection of each Wi-Fi standard impacts the user experience, so a summary of the standards is included.

2.4GHz vs. 5GHz

Wi-Fi networks operating at 2.4GHz allow for 11 channels in the United States. However, due to channel interference considerations, only channels 1, 6, and 11 should be used in a network design.

5GHz signals do not penetrate walls and other barriers as well as 2.4GHz signals, which results in a smaller coverage area. Therefore, 5GHz networks may be preferred when you design for a high density of devices in an enclosed space, such as in classrooms. The number of channels available in the 5GHz band varies among vendors of access points and from country to country, but at least 8 channels will always be available.

5GHz channels are nonoverlapping, which is a significant departure from the three nonoverlapping channels available in the 2.4GHz band. When designing a Wi-Fi network for a high density of iOS devices, the additional channels provided at 5GHz become a strategic planning consideration.

IEEE 802.11b/g

If devices that only support the 802.11b or 802.11g standards are required to participate on the network, 802.11b/g should be included in the Wi-Fi network design.

802.11b provides data transfer speeds of up to 11Mbps, while 802.11g provides data transfer speeds of up to 54Mbps. Under ideal conditions, the actual data throughput, or the actual speed at which devices will exchange information, is about half the data rate. Both technologies are implemented in the 2.4GHz band, the same band at which many cordless phones, microwaves, and other wireless devices operate. Note that when both 802.11b devices and 802.11g devices are using the same wireless network, the 802.11b devices cause reduced data throughput for the faster 802.11g clients.

IEEE 802.11a

In contrast to 802.11b/g, the 802.11a standard operates in the 5GHz band. Most notebook computers support this band, but many smaller mobile devices only support 2.4GHz Wi-Fi.

Transfer speeds and data throughput when using 802.11a are similar to those with 802.11g.

IEEE 802.11n

The newest 802.11 standard is 802.11n. This standard is capable of transmit speeds of up to 600Mbps. To accomplish this task, several technologies are used.

802.11n can use either the 2.4GHz or 5GHz band and is compatible with the 802.11a/b/g standards, so older devices can share the same network as the newer 802.11n devices.

802.11n supports several operating modes:

- 802.11n @ 5GHz
- 802.11n @ 2.4GHz
- 802.11n + 802.11a @ 5GHz

- 802.1n + 802.11b/g @ 2.4GHz
- 802.1n + 802.11g @ 2.4GHz
- 802.1n + 802.11b @ 2.4GHz

Most multi-radio access points allow any combination of the above modes.

The 802.11n standard uses a technology called Multiple Input Multiple Output (MIMO) to achieve higher speeds. MIMO supports transmitting multiple streams of data, called spatial streams, simultaneously. To take advantage of these spatial streams, both the access point and client must have multiple radios and antennas. Mac products support multiple spatial streams while iOS devices support a single spatial stream.

HD40, commonly referred to as wide channels or channel bonding, is another technology used to accomplish faster transmit speeds. Approximately double the amount of data can be transmitted through this single but wider channel. Nonbonded channels are called HD20. Channel bonding should not be used in the 2.4GHz band because there are only three nonoverlapping channels available. Thus, many access point vendors do not allow configuring channel bonding when using the 2.4GHz band. iOS devices support HD20 while Mac products support channel bonding.

Wi-Fi Standards Support in Apple Products

Support in Apple products for the various Wi-Fi specifications are listed below. The list includes the following details:

- 802.11 compatibility: 802.11b/g, 802.11a, 802.11n
- Frequency band: 2.4GHz or 5GHz
- MCS index: The Modulation and Coding Scheme (MCS) index defines the actual data rate at which 802.11n devices can communicate. See the MCS index table listed later in this appendix for more information.
- Channel bonding: HD20 or HD40
- Guard interval (GI): The guard interval is the space (time) between symbols or characters of information transmitted from one device to another. The 802.11n standard defines a short guard interval of 400ns that allows for faster overall throughput, but devices may utilize a long guard interval of 800ns.

iPhone 4S

802.11n @ 2.4GHz

802.11 b/g

MCS Index 7 / HD20 / 800ns GI

iPhone 4

802.11n @ 2.4GHz

802.11 b/g

MCS Index 7 / HD20 / 800ns GI

iPhone 3GS

802.11 b/g

MCS Index 7 / HD20 / 800ns GI

iPad and iPad 2

802.11n @ 2.4GHz and 5GHz

802.11a/b/g

MCS Index 7 / HD20 / 800ns GI

iPod touch (4th Generation)

802.11n @ 2.4GHz

802.11 b/g

MCS Index 7 / HD20 / 800ns GI

MacBook Pro, MacBook Air, and MacBook

802.11n @ 2.4GHz and 5GHz

802.11a/b/g

MCS Index 15 / HD40 / 400ns GI

MCS Index 23 / HD40 / 400ns GI (early 2011 or later MacBook Pro)

MCS Index

MCS Index	Spatial streams	Modulation	Coding rate	Data rate (in Mbps) (GI = 800ns)		Data rate (in Mbps) (GI = 400ns)	
				20MHz	40MHz	20MHz	40MHz
0	1	BPSK	1/2	6.5	13.5	7.2	15.0
1	1	QPSK	1/2	13.0	27.0	14.4	30.0
2	1	QPSK	3/4	19.5	40.5	21.7	45.0
3	1	16-QAM	1/2	26.0	54.0	28.9	60.0
4	1	16-QAM	3/4	39.0	81.0	43.3	90.0
5	1	64-QAM	2/3	52.0	108.0	57.8	120.0
6	1	64-QAM	3/4	58.5	121.5	65.0	135.0
7	1	64-QAM	5/6	65.0	135.0	72.2	150.0
8	2	BPSK	1/2	13.0	27.0	14.4	30.0
9	2	QPSK	1/2	26.0	54.0	28.9	60.0
10	2	QPSK	3/4	39.0	81.0	43.3	90.0
11	2	16-QAM	1/2	52.0	108.0	57.8	120.0
12	2	16-QAM	3/4	78.0	162.0	86.7	180.0
13	2	64-QAM	2/3	104.0	216.0	115.6	240.0
14	2	64-QAM	3/4	117.0	243.0	130.3	270.0
15	2	64-QAM	5/6	130.0	270.0	144.4	300.0
16	3	BPSK	1/2	19.5	40.5	21.7	45.0
17	3	QPSK	1/2	39.0	81.0	43.3	90.0
18	3	QPSK	3/4	58.5	121.5	65.0	135.0
19	3	16-QAM	1/2	78.0	162.0	86.7	180.0
20	3	16-QAM	3/4	117.0	243.0	130.0	270.0
21	3	64-QAM	2/3	156.0	324.0	173.3	360.0
22	3	64-QAM	3/4	175.5	364.5	195.0	405.0
23	3	64-QAM	5/6	195.0	405.0	216.7	450.0
24	4	BPSK	1/2	26.0	54.0	28.9	60.0
25	4	QPSK	1/2	52.0	108.0	57.8	120.0
26	4	QPSK	3/4	78.0	162.0	86.7	180.0
27	4	16-QAM	1/2	104.0	216.0	115.6	240.0
28	4	16-QAM	3/4	156.0	324.0	173.3	360.0
29	4	64-QAM	2/3	208.0	432.0	231.1	480.0
30	4	64-QAM	3/4	234.0	486.0	260.0	540.0
31	4	64-QAM	5/6	260.0	540.0	288.9	600.0

Appendix B—Wireless Security

Over time, several technologies have been developed to protect and secure Wi-Fi networks. Some of the early technologies include WEP (Wired Equivalent Privacy), LEAP (Lightweight Extensible Authentication Protocol), device filtering by MAC address, and hiding the network SSID. While using these technologies provided some level of Wi-Fi network security at the time, all of these technologies are now considered insecure and can easily be compromised.

Fortunately, current Wi-Fi standards such as WPA and WPA2 provide technologies for network authentication and encryption to secure data. If these security standards are in place, there is no benefit in implementing any of the legacy technologies.

IEEE 802.11i, WPA, and WPA2

WPA (Wi-Fi Protected Access) and WPA2 refer to a suite of tests that ensure compatibility between various Wi-Fi devices. The actual Wi-Fi security standard is defined by the IEEE in 802.11i. In general, this specification defines two areas of network security: authentication for obtaining access to the network and encryption of data itself as it passes from one Wi-Fi device to another. WPA and WPA2 are commonly used to define which 802.11i options are enabled on the network. The main difference between WPA and WPA2 is the strength of data encryption. WPA2 is preferred over WPA.

PSK vs. Enterprise

Access to a WPA or WPA2 network can be secured with a single password for all users or by providing an individual credential to each user or device. This credential could be in the form of a user name and password or a PKI identity (certificate). Using a single password for all devices is referred to as a Pre-Shared Key (PSK). The enterprise version refers to the implementation of 802.1x for individual credentials assigned to each user or device. Regardless of the method used for network authentication and encryption, be sure to use WPA or WPA2 for a secure Wi-Fi network.

Broadcast or Hidden SSID

A Wi-Fi network name is called the SSID (Service Set ID). To join a specific wireless network, the user selects the SSID for the desired network from a list of SSIDs being broadcast within the range of the Wi-Fi device. However, it's also possible to hide the SSID so that it does not show up in searches. While there may be a perception that hiding the SSID is more secure than broadcasting the SSID, in reality there is very little security benefit.

Hiding the network SSID means that a user won't see the network in a list of networks within range of the computer, but it would take a potential hacker only a few seconds to get the name of the network simply by using a computer to listen to information being transmitted by Wi-Fi devices already associated with the hidden SSID. This is possible because even with a hidden SSID, the name of the network is transmitted unencrypted within the data.

More important are the practical implications of a hidden SSID. For a Wi-Fi device to rejoin a hidden SSID, it must first locate access points offering that SSID. However, because the SSID is hidden, the Wi-Fi device must visit every known channel and broadcast to see if the hidden SSID exists on that channel. After broadcasting, the computer must wait a certain amount of time for responses. If the client has multiple saved hidden SSIDs, it must broadcast on each channel for each of the SSIDs and wait for a response after every channel broadcast for every SSID.

When finding a broadcasted SSID, the computer visits each channel and simply listens for the SSIDs that exist on that channel. It doesn't matter how many saved broadcast SSIDs might exist on a computer, the computer still only has to listen one time on each channel to find them.

Simply put, it's harder for a Wi-Fi device to rejoin a hidden SSID than a broadcast SSID, and there's very little security benefit in hiding the SSID. iOS devices tend to physically move frequently, so hidden SSIDs may delay their network association time.

Appendix C—Supporting Bonjour

Information that is simultaneously transmitted across the network to a specific group of devices at the same time is called multicast traffic. A special case of multicast traffic in which the information is simultaneously transmitted to all network devices is called broadcast traffic. These methods of transmitting data are used in various ways. For example, when a computer obtains an IP address using DHCP, it uses a broadcast to request an IP address. By using a broadcast, it insures that the DHCP server will receive the request because the broadcast goes out to all computers.

Apple uses a technology called Bonjour to allow users to find devices and services on a network. Computers and devices with Bonjour automatically broadcast their own services and listen for services being offered by others. A computer might see a printer available for printing, a shared iTunes playlist, an iChat buddy available for video conferencing, or another computer sharing files. iOS devices use Bonjour to discover AirPrint compatible printers and AirPlay compatible devices such as Apple TV. Even Windows computers can take advantage of Bonjour if iTunes is installed. Bonjour works with standard connection technologies, including Ethernet and Wi-Fi (802.11). It uses the standard, ubiquitous IP networking protocol for its connections, the same protocol that runs the Internet itself.

Multicast traffic, especially broadcast traffic, can also consume network bandwidth very quickly. Imagine if every time a network device transmitted something on the network the information was sent to every other network device. Because wireless devices receive data at different speeds, broadcast traffic would be broadcast at the speed of the slowest client. Excessive broadcast traffic can cause what is called a "broadcast storm" and make the network inaccessible. Wi-Fi networks are especially vulnerable to this.

Work with a Wi-Fi network provider to create a network design that allows for multicast traffic efficiently and in a way that doesn't adversely affect other network clients. Unnecessary broadcast traffic can be reduced with configuration changes on the client devices. This reduces the amount of Bonjour service registrations on the network, and therefore reduces the overall amount of broadcast traffic on the network. Changes can also be made to the network infrastructure, including access points, to allow or filter broadcast traffic.

- Learn more about Bonjour
  www.apple.com/support/bonjour