How Cisco IT Is Providing Corporate Bring Your Own Device (BYOD) for the Enterprise

Cisco IT BYOD program simplifies business communications, increasing productivity and allowing employees to choose their own devices.

EXECUTIVE SUMMARY

CHALLENGE

- Growing employee demand for support of popular smartphones and digital tablets
- Need to reduce IT costs
- Provide a secure, scalable, and easy to use solution

SOLUTION

- Plan governance, security and support policies
- Reduce corporate-paid accounts while allowing corporate access from employees' personal devices
- Create self-support community within WebEx Social

RESULTS

- Increased user productivity: US$300 million
- Eliminated US$500,000/year spend and $850,000 device upgrade spend
- Reduced per-user support costs 25 percent

LESSONS LEARNED

- Plan for rapid growth and escalating user needs
- Provide resources for user self-support

NEXT STEPS

- Automate application and service delivery using eStore
- Support new secure mobile cloud services

Background

Since 2009, Cisco changed how it supports personal mobile phones and their associated service plans when used by employees for business purposes. This change resulted in far wider employee use of smartphones for business use (see Figure 1), increasing employee productivity, satisfaction, and flexibility. At the same time, a different governance and support model, the Bring Your Own Device (BYOD) program, saves Cisco money. The BYOD Program was the first phase of Cisco ITs "Any Device" initiative, with the goal of providing Cisco employees secure access to corporate resources from any location, any device.

In the early 2000s, smartphones that could handle voice and data enabled Cisco IT to offer mobility services. Mobility Services helped increase productivity to sales, customer support, and executive-level employees by giving them access to their business email, calendars, and contacts, as well as access to internal web content from wherever they were, using these mobile devices.

Initially, Cisco paid for, owned, provisioned, and supported a limited number of primarily Blackberry or Nokia mobile devices for eligible employees. Today, however, consumer smartphones are the prevailing mobility device and pose a new challenge for Cisco IT.

In the earlier strategy, an employee would request a specific mobile device from a limited set of devices. Cisco IT would provision specific services to that device, including a pre-negotiated service providing voice, messaging, and data plan, delivering a predefined user experience.

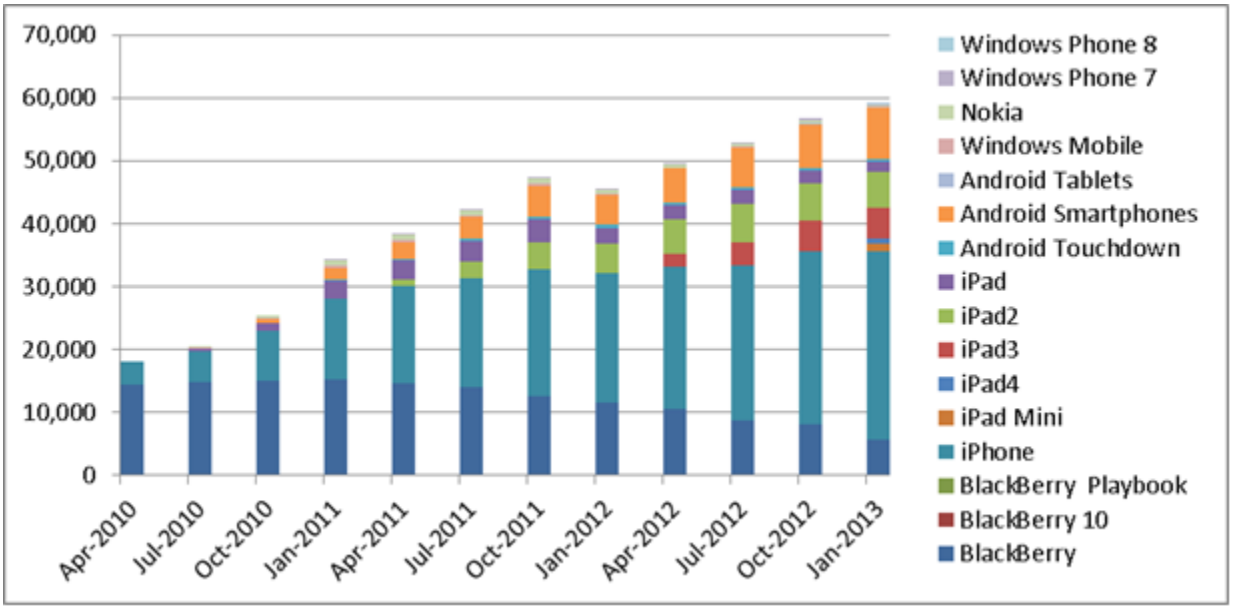
Challenge

Starting in 2009, two major business drivers prompted Cisco IT to review and change key aspects of its mobility services strategy.

First, the global economic downturn forced Cisco to cut expenses and review the ongoing costs of Cisco-paid mobile phone services. Cisco evaluated factors such as which employees were entitled to company-paid mobile phones and service plans, the number and type of mobile devices that Cisco IT would support, and an internal budget charge for employee use of the Cisco IT mobility services.

Second, consumer devices such as the Apple iPhone became more sophisticated, powerful, and user-friendly, and their use became far more popular among Cisco employees than the devices that Cisco IT made available at the time. Cisco employees demonstrated that their mobile devices enabled them to be more productive (internal studies showed that on average the mobile device user gained at least 15 minutes of productive time per day). The emergence of tablet devices such as the iPad also increased employee interest in mobility services. Cisco IT initiated and established ways to satisfy employee needs for flexibility and convenience.

Figure 1. Growth of Mobile Device Numbers at Cisco



Three major challenges arose to enabling a mass expansion of the mobility program onto a variety of new platforms:

First, with such a rapidly growing number of employees requesting the use of new (and increasingly expensive)

mobile devices and service plans, how can Cisco IT support employees while cutting costs?

Second, how can Cisco IT ensure that the solution is secure? With so many types of devices and service providers, how can each of the hundreds of possible platforms be secured?

Third, how can Cisco IT sustain all these new devices? Imposing limited phone models and service plans enables IT to consolidate and reduce support staff and processes; opening up the mobility program to hundreds of different device and service provider combinations might nearly be impossible to support cost effectively.

Solution

The growing popularity of smartphones and tablets prompted Cisco IT to transform its mobility strategy.

Governance

From supporting only a small number of devices and a limited list of services to implementing a BYOD strategy, Cisco IT enables each employee to choose among many different devices and multiple user services – as long as they pay for the device themselves (see Table 1).

> "The demand among employees for connecting mobile devices to our network is getting bigger and becoming more complicated. Our model for delivering mobility services is allowing us to handle this kind of growth."
> **– Brett Belding, Manager, Cisco IT Mobility Services**

In the new strategy, employees select their own device and then request access to a type of mobility service, which is approved and paid for by the employee's department. Cisco IT provisions that service and allows the employee to connect to it natively from multiple devices, such as a smartphone and a tablet. The employee simply configures additional devices as required. Activating multiple devices does not result in additional internal service charges to the employee's department, and approval from the employee's manager is not required.

Table 1. Governance: Mobility Options at Cisco

	Device	Service
Original Option	• Paid for by Cisco if approved by VP • One of a limited selection of BlackBerry or Nokia models • Only available if the employee's job requires use of a mobile device • Employee's department is charged for device lease	• Paid for by Cisco if approved by VP • With one or a few service providers / vendors within each country • Service plans negotiated by Cisco • Employee's department is charged for monthly service fees
BYOD, Cisco-paid service	• Selected and paid for by the employee if approved by manager • Not available in some countries in Europe, where regulations require that all work equipment is provided by employer • Employee's department is charged for a small fee for service connection and support	• Paid for by Cisco if approved by VP • With one or a few service providers / vendors within each country • Service plans negotiated by Cisco • Employee's department is charged for monthly service fees
BYOD, Employee-paid service	• Selected and paid for by the employee if approved by manager • Not available in some countries in Europe, where regulations require that all work equipment is provided by employer • Employee's department is charged for a small fee for service connection and support	• Selected and paid for by the employee • Employee can select any service plan with any major provider. In some countries, employee can select from a Cisco service plan with negotiated discounts.

Employee Eligibility and Who Pays for What

To control costs, Cisco established corporate-wide policies that define an employee's eligibility for company-paid mobile devices and associated service plans. In most cases, the employee pays for the mobile device and its associated service plan. However, this corporate policy can be modified by each Cisco department or regional / country organization, as needed, to match local business or legal requirements. In general, employees required to use a mobile device for their job can select from a small range of basic, company-provided devices.

For a small number of eligible employees, Cisco covers the cost of monthly mobile service plans as defined by company policy. (In most cases, the employee must purchase the mobile device.) Requests for a company-paid

mobile account must be approved by a vice president to control the costs of mobile communications.

“At an average cost of [US]$120 per month per line, mobile service charges can quickly become a very large annual expense,” says Brett Belding, manager, Cisco IT Mobility Services. “With this policy, only employees whose job roles really justify a company-paid mobile account are likely to request approval at the VP level. This helps restrict the number of accounts that exist primarily for employee convenience.”

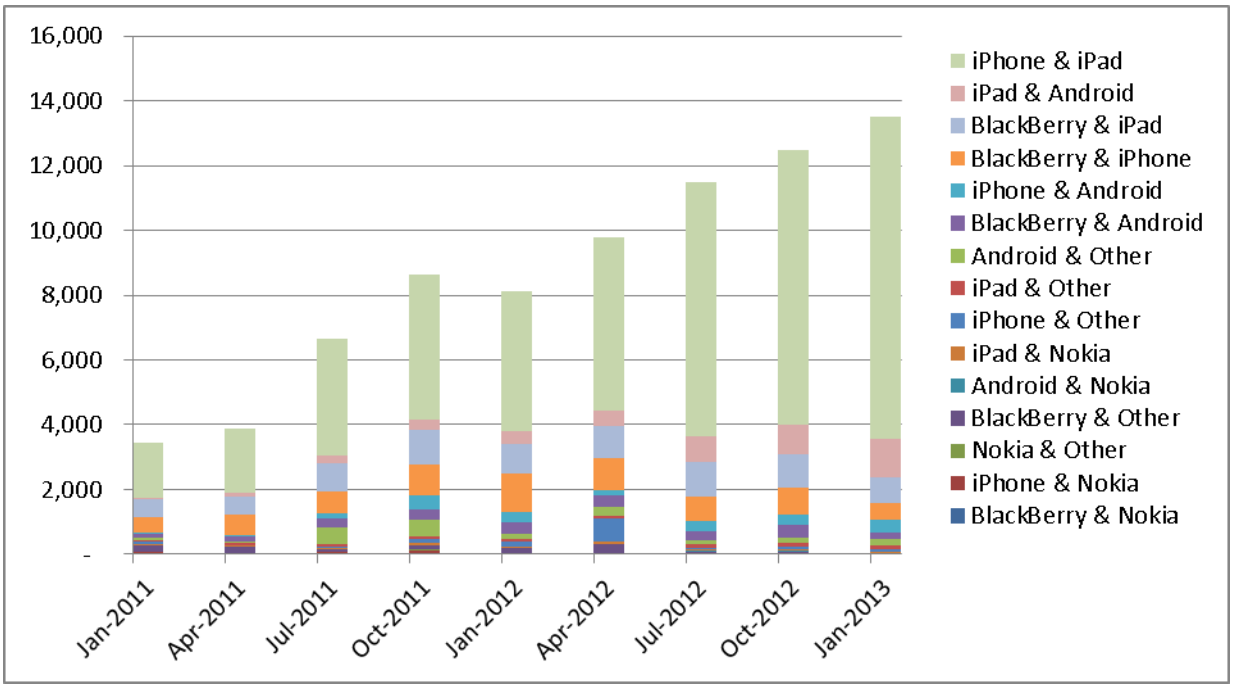
Employees who are eligible for Cisco-paid smartphone service are added to the Cisco corporate plan (where applicable), and Cisco is billed directly for the employee’s monthly mobile service charges. Cisco has negotiated contracts with mobile carriers worldwide to reduce costs. Cisco IT also notifies employees of calling plans available for people who expect to be working entirely in one country, or roaming for lesser or greater lengths of time. To help track problem bills, managers receive reports showing exceptionally large service bills for individual employees. Managers can determine how best to solve problems with different situations or different calling plans.

Employees who are not eligible for Cisco-paid mobile service can request approval from their manager (which is usually granted) to access the Cisco network with their personal smartphone and personal-paid service plan. In this case, the employee pays for any apps, family plan, termination fees, overage charges for call minutes or data usage, and additional mobile services. These options are not allowed on a Cisco corporate-paid mobile account.

Cisco IT also charges the employee’s department a small amount for using mobility services. These monthly, per-user charges offset the costs incurred by Cisco IT for developing, maintaining, and delivering the mobility services. The charges are adjusted annually, based on Cisco ITs actual costs for the current infrastructure and to allow for ongoing growth in the number of users.

Today, most Cisco employees choose smartphones as their primary mobile device, and many use tablets as a secondary mobile device. As of early 2013, more than 35 percent of Cisco employees with mobile services carry two mobile devices in addition to their standard laptop, a trend that is increasing (see Figure 2); and a growing number of employees carry three or more devices (although frequently for research or application development and testing).

Figure 2. Growth of Two Mobile Devices Registered to Single Employee



Approved Mobile Devices

During the early years of offering mobility services, Cisco IT performed extensive testing on individual mobile devices before adding them to the approved list. However, the support model proved impossible with the large and increasing number of mobile devices available over time.

Today, Cisco IT primarily approves new mobile devices based on the operating system, for example, Apple iOS, Android, and BlackBerry.

“It’s the operating system that provides most of the device capabilities like email and calendaring that we’re concerned about,” says Paul Clements, Cisco IT technical lead for Mobile Solutions. “If it’s not a BlackBerry device, we also consider whether the device supports the security policies we require such as using Microsoft ActiveSync technology, which we now use for synchronizing a user’s email, calendar, and contact list between a mobile device and our Microsoft Exchange environment.”

As of mid-2011, more than 50 different mobile devices, including smartphones and tablets, were on the Cisco IT validated list based on their wide availability and compliance with Cisco IT security requirements. Not all devices were considered entirely secure.

“Currently, BlackBerry and Apple devices running the latest Apple iOS version provide the device security necessary for access to the broadest array of Cisco IT mobility services, including data and applications on the corporate intranet,” says Belding. “Devices based on other operating systems can access a smaller subset of user

features, or we restrict them to accessing only the user's corporate email, calendar, and contacts."

Even for access to these basic services, Cisco IT requires that the device meets certain security requirements.

Mobile Access Services

The Mobile Mail Essentials service offers direct, secure access to Cisco email servers over a mobile carrier or wireless LAN connection and, in most cases, uses the device's native functionality for email, calendar, and contacts. To deliver the Mobile Mail Essentials service, Cisco IT uses the Microsoft ActiveSync platform, which is supported by many mobile device operating systems. BlackBerry users are supported by the BlackBerry Enterprise Server (BES) infrastructure, which is specific to that operating system.

Not all devices can support all service features. For example, only some devices provide access to 802.11 wireless LAN connections; this access is required to make calls over a wireless LAN. Other devices cannot support a VPN client. To help user purchases, Cisco IT guides employees with a menu of popular mobile devices that shows which devices can support which features and meet the minimum security requirements for the Cisco environment. Still, Cisco IT has a goal of increasing the services offered to each approved device, in part by leveraging the Cisco AnyConnect® VPN Client and third-party solutions for managing mobile devices.

Cisco IT provides the mobility services listed in Table 2, which are based on the device's security level and capabilities.

Table 2. Cisco IT Mobility Services Set

Feature	Description
Single-Number Reach	Employee has a single work phone number. Dialing that number rings the work phone, then the mobile device; unanswered calls are recorded by the work voicemail system (Unity Connection). Single-Number Reach is a function of the Cisco Unified Communications Manager and works for any working mobile phone.
Mobile Mail Essentials	Employee can access corporate email and calendar and contact lists from any smartphone, using Microsoft ActiveSynch.
Cisco WebEx® Conferencing	Employees from any video-capable smartphone can join Cisco® WebEx conference meetings. WebEx conferencing is a cloud service and does not require intranet access.
Cisco Jabber™	Employees with smartphones can use corporate IM, Presence, Voice and Video, and Visual Voicemail from any location, both over the internal enterprise wireless LAN or over the vendor's mobile data service
Intranet Access and Applications	Employees with a smartphone certified as "secure" by Cisco IT can use Cisco AnyConnect VPN to access the corporate intranet and internal tools, including Cisco WebEx Social and the many Cisco eStore applications (e.g., My Expenses, My PTO, and My Approvals). Cisco eStore is a single place where employees can conveniently find all the IT services and apps they need on any device (Figure 7).

Carrier Services and Management

Mobility services are available to all Cisco employees, regardless of whether or not Cisco pays the carrier invoice. Employees who are not eligible for a corporate paid service can request access for email, calendar, and contacts as well as VPN and the intranet on their own devices. This offer extends to multiple devices including tablets.

Cisco works with its global network of carriers to optimize spend. With a data-hungry workforce that frequently travels, Cisco needs innovative solutions to delicately balance spend with productivity. Employees are encouraged to use Wi-Fi wherever possible when travelling. Cisco also works with its carriers to develop pooled data plans, where IT can manage the fleet as a whole and avoid the costs associated with overage charges and avoid under-utilization.

Where possible, Cisco uses “split billing,” where Cisco pays for the usage costs directly, and employees pay the carrier directly for their choice of handset.

Security

Providing secure BYOD solutions warrants three considerations:

- Securing the mobile devices themselves, their apps, and their data, to make these devices safeguarded from being used or read if they are lost or stolen.
- Securing the network architecture, to protect the devices and data from external threats (malware) and to protect the network against intrusion by non-authorized devices.
- Securing the end user, educating employees about their responsibilities to keep Cisco secure while using their mobile device(s), and helping them avoid common security mistakes.

Securing Mobile Devices

The type and strength of security measures in a mobile device present two critical concerns for any mobility service-offering IT department. First, mobile devices store proprietary information such as contacts and emails. If the device is lost or stolen, information should not be accessible to others. Second, since email and web applications contain confidential information, users and their mobile devices must be authenticated before they can access internal resources. These concerns can be addressed by two types of security: securing the device’s content and securing the device’s access to the corporate network (see Figure 3).

Figure 3. Cisco IT Security Design for Mobility Services

“As a principle for mobile device security, the more the device can access, the more security we require,” says Jason Freeth, mobility architect, Cisco IT.

To access mobile services in the network edge (shown in the outer ring in Figure 3), the mobile device must meet the security requirements listed below before it is considered a trusted device by Cisco IT. A device that does not comply with these basic requirements cannot connect to the Cisco network:

- Ability to remotely wipe the device if it is lost or stolen
- Minimum four-digit password for accessing the phone's content and applications
- Password re-entry required after 10 minutes of inactivity

Accessing mobile services within the Cisco core network (shown in the inner ring in Figure 3) requires two additional security measures: use of the Cisco AnyConnect VPN Client and built-in device encryption.

Additionally, the user must register the phone number and / or unique device identifier (UDID) for the mobile device with Cisco IT. Only registered devices can access internal services. Device registration also allows Cisco IT to apply encryption to content (data at rest) in the device and perform device management tasks such as checking the inventory of software versions and device status.

“These security requirements protect the device itself, but they can also help prevent a third party from gaining unauthorized access to Cisco applications and confidential information,” says Clements. “In addition, we have

defined which services are available to users based on their device, which means they can't access anything their smartphone or tablet can't protect."

PRODUCT LIST

Infrastructure and Cloud Services
- Cisco Identity Services Engine
- Cisco Cloud Web Security
- Cisco Email Security
- Cisco Web Security
- Mobile Device Manager
- Cisco Prime™ Service Catalog
- Cisco Process Orchestrator

Unified Communications
- Cisco Unity® Connection

Video and Collaboration
- Cisco WebEx
- Cisco AnyConnect VPN client

Cisco Mobility Applications in eStore
- Cisco AnyConnect for Mobile devices
- Cisco Jabber for Mobile devices
- Cisco WebEx Social for Mobile devices
- Many others in eStore

During the user-driven setup process, a Rules of Use document presents security practices that require users to view and acknowledge the rules to receive approval for mobility services. This document covers security issues such as not "jailbreaking" the mobile device (that is, obtaining root level or command line access), protecting confidential data, and regularly updating the device's operating system software.

Securing the Network Architecture:

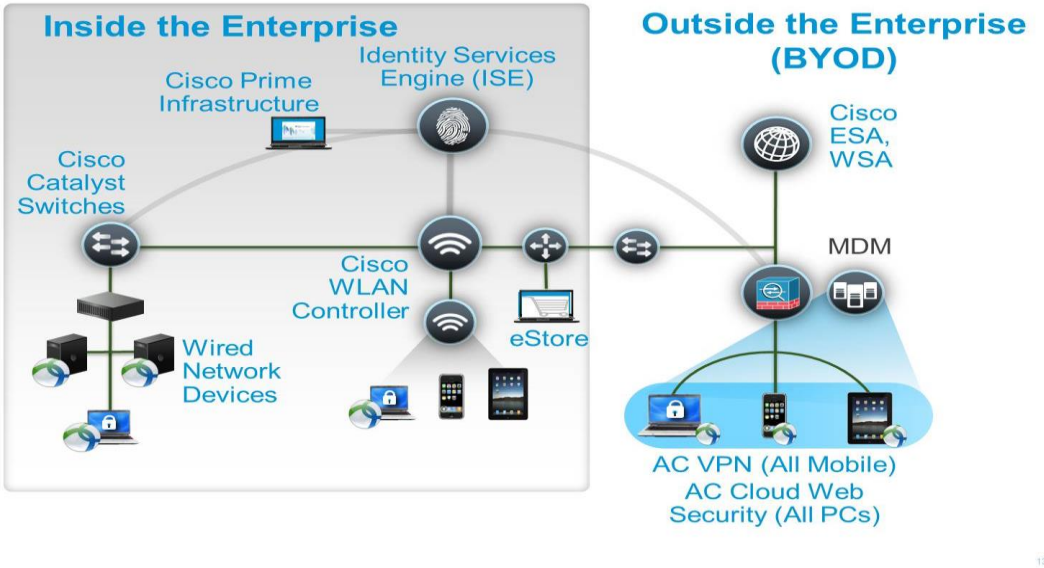
Cisco IT needs to deliver secure, cohesive, and automated network security solutions to users whether they are on campus or off. Network protection comes from a variety of network resources, and most of them are part of the network already guarding the wired and wireless networks inside Cisco. Cisco widens its scope to include mobile devices. However, some parts of this architecture are specific to the mobile environment (see Figure 4).

Some of the components in this architecture include:

Mobile Device Manager (MDM) handles device posture and app delivery. The MDM checks data and configuration settings when it attempts to connect to the Cisco network, investigating if it has been registered within Cisco, and if it retains secure posture (running on the minimum operating system, using digit PIN, 10-minute timeout, remote wipe enabled, contents encrypted, anti-malware enabled, and so on).

Cisco AnyConnect Secure Mobile Client runs on several mobile devices at Cisco, including iPhones and iPads (as well as all employees' PC and Mac laptops). Using IPsec Internet Key Exchange (IKEv2) and Secure Sockets Layer (SSL) protocols, the client supports a secure connection back to Cisco. Cisco AnyConnect Secure Mobile Client connects through to the Cisco Adaptive Security Appliance (ASA) 5500 in the Cisco network to authenticate a user attempting to access the intranet. The client encrypts and secures the mobile data stream against being read or compromised.

Figure 4. Cisco IT Security Architecture for BYOD and Wired and Wireless Access



Cisco Web Security Appliance (WSA) screens all Cisco web access outside of Cisco, from any device using Cisco AnyConnect Secure Mobility Client. The WSA evaluates websites by both reputation and content. It then blocks or monitors access, or blocks or monitors specific features such as chat, messaging, video, and audio, based on Cisco internal security policies. By using these policies, Cisco IT blocks about 2 percent of website requests, the equivalent of 6 to 7 million site requests blocked per day. Most of these requests are blocked due to web reputation information, but 2 percent of the requests are blocked because of malware such as Trojans or Trojan downloaders (more than 500,000 malware downloads are blocked per day).

Cisco Email Security Appliance (ESA) screens all Cisco mail traffic from outside Cisco to any device, including smartphones. The Cisco ESA blocks email from known spam providers, or by spam content and other email irregularities. Of the 5.6 million emails Cisco gets per day, almost two-thirds are blocked. About 15 percent of email with some marketing content are allowed through, but is marked “Marketing” or “Possible Spam” by the ESA server.

Cisco Identity Services Engine (ISE) controls access to internal wired and wireless resources based on the end user and end device by control point for identity, access control, and device security across wired, wireless, and VPN networks. The ISE integrates with the Cisco MDM solution to help ensure that all mobile devices comply with the security policy before they are allowed on the network (for example, is the device registered to the MDM, does it have the four-digit PIN and the 10-minute or less timeout, is the disk encrypted, and has the device been rooted or jailbroken). ISE with the MDM solution also performs ongoing posture checks to ensure that devices remain compliant. They enforce existing internal Cisco security policies restricting user access to different secured content repositories based on how they arrive in the network and from what devices. The MDM identifies which devices are compliant, while the ISE enforces these rules by denying access to non-compliant devices. BYOD devices attempting to access internal resources will also be restricted by Active Directory-based strong access control that

is already part of the Cisco infrastructure.

Cisco Prime™ Infrastructure provides complete end-to-end network visibility across the wireless and wired network, from any device (including mobile clients) to the data center. This visibility enables Cisco IT to understand, troubleshoot, and fix application-, services-, and end user-related issues.

Cisco Prime Service Catalog and Cisco Process Orchestrator gives Cisco employees the ability to download a growing suite of mobile apps through the internal Cisco eStore. (Cisco eStore is a single place where employees can conveniently find all the IT services and apps they need on any device.) This solution automates the provisioning process, screens for eligibility, generates approval requests, provisions the service, and manages the service lifecycle.

Securing the End User: Training and Communication

Code of Business Conduct: Every Cisco employee, once a year, must review the Cisco Code of Business Conduct (COBC), which defines ethical behavior at Cisco. Not following the guidelines in the COBC can result in termination of employment. All employees must certify that they have reviewed, understood, and agreed to abide by it. Part of that code, to follow the "Acceptable Use Policy" for Cisco computing devices (including laptops and smartphones), states:

"Unless otherwise prohibited by local laws and regulation, Cisco has the right to require security controls on all electronic and computing devices used to conduct Cisco business or interact with internal networks and business systems, **whether owned or leased by Cisco, the employee, or a third party**."

"You are responsible for ensuring the protection of electronic and computing devices used to conduct Cisco business or interact with internal networks and business systems, whether owned or leased by Cisco, the employee, or a third party. Unattended devices must be properly secured. You have a responsibility to promptly report the theft or loss of electronic and computing devices used to conduct Cisco business."

"All computing devices must be secured with a password-protected screensaver with the automatic activation feature set to 10 minutes or less. You must lock the screen or log off when the device is unattended."

"You may not circumvent or interfere with security controls, including but not limited to authentication controls, corporate device management software, or security system software."

When Cisco employees order their first Cisco service for their mobile device, they are required to review and accept the **Cisco Mobility Rules of Use**, stating:

"Cisco reserves the right to delete data from your Cisco-enabled mobile device, either directly or "over the air," if Cisco confidential information is deemed likely to be compromised. Further, it is likely that any personal data, third-party applications or operating system files stored on the device would be deleted in this process as well. You acknowledge and agree that Cisco shall bear no liability for loss or damage resulting from such action."

Employees who do not agree with these rules of use do not get access to Cisco services.

Internal guidance about keeping mobile devices secure is provided to employees. In addition to support from Cisco IT, the Mobility community on the internal Cisco WebEx Social platform provides ongoing discussion forums, as well as training, including user guides and best practices, recorded webinars, and short training demo videos in

Show and Share. Employees signed up for BYOD will, as needed, receive email announcements (vulnerability announcements, security advisories, and more) that are relevant to their current service.

Support

Cisco employees need a varying level of support throughout the service lifecycle:

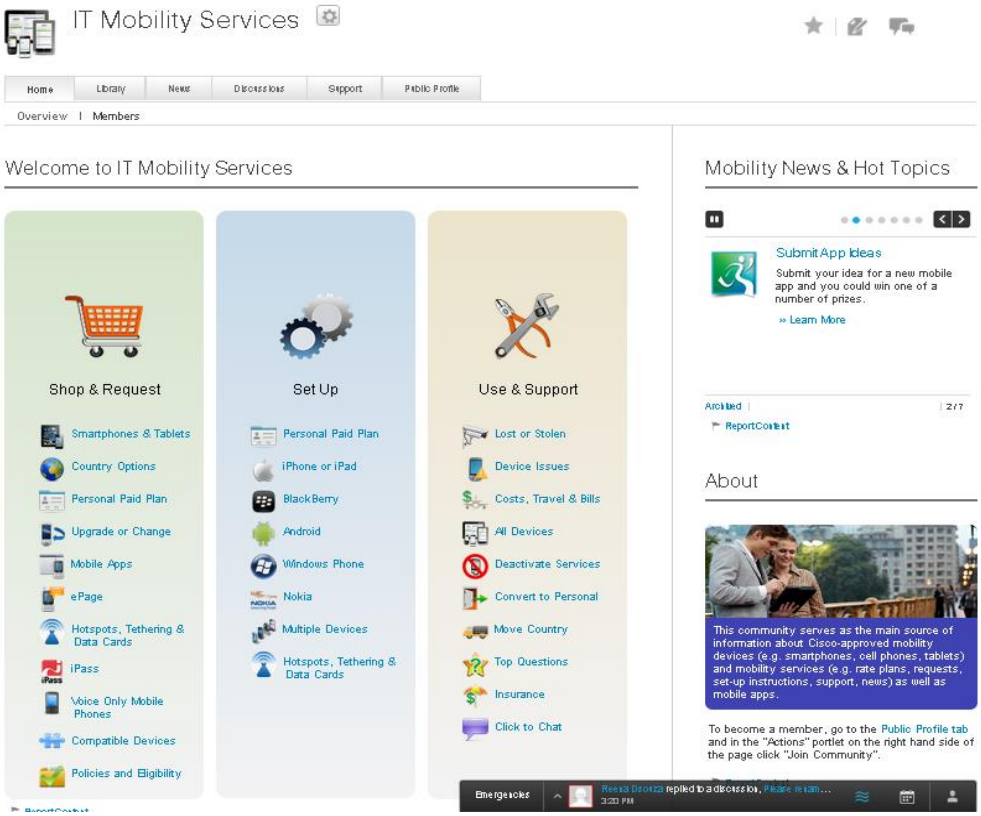
- Choosing the right device and the right service plan
- Acquiring management authorization
- Signing up for and installing new services
- Supporting services on multiple devices
- Troubleshooting failures problems
- Managing unexpected costs (especially while traveling)
- Dealing with lost or stolen phones
- Upgrading to a new phone

Cisco IT provides most user support through the internal online Mobility Services community on WebEx Social. Employees can use this community (see Figure 5) for most of the common tasks listed above as well as updating and improving topic areas.

“By encouraging user participation, we are building a user community where they can share ideas and recommendations and help us to quickly identify needed new services,” says Belding.

While employees are encouraged to use self-support, they can still open a case online, or even call the help desk for time-sensitive issues or issues that require a high level of expertise. Most employees prefer the speed and efficiency of self-support, as shown by the Cisco per-device case numbers dropping by more than 50 percent.

Figure 5. IT Mobility Services Community for Self-Service Information, Service Procurement, and Support



Results

Enabling Cisco employees to use their own mobile devices at work has a tremendous impact on the culture at Cisco. Employees embraced mobility and BYOD and are enjoying the productivity benefits from the ability to work anywhere.

Growth and Satisfaction

Mobility services are used by Cisco employees in more than 70 countries, with the largest number of users in the United States and working in sales, customer support, and company operations roles.

As of mid-2013, Cisco IT provides mobility services for more than 66,000 mobile devices, an increase of almost 40 percent over the last year. This dramatic rate of growth does not appear to be slowing (see Figure 1). The growth stems from employees researching and buying mobile devices, apps, and services to help them make their jobs more productive, more flexible, and more satisfying.

The demand for smartphone support at Cisco will continue to grow. Today, about 35 percent of the mobile devices

connecting to the Cisco network are secondary devices for the employee. The most popular device combinations are an iPhone or BlackBerry smartphone with a tablet. Some employees also connect using their company-paid BlackBerry phone and their own personal-paid smartphone (see Figure 2). A few employees have three or more devices (usually for application testing).

While iPhones and iPads are the most popular devices, the number of Android devices has grown rapidly in the past two years and is near that of iPads. Outside of the smartphones and tablets, around 7000 of these devices are still voice-only phones and pagers that are typically passed within a team of on-call employees. The number of voice-only devices is declining as they are replaced by smartphones when service contracts are renewed.

“The demand among employees for connecting mobile devices to our network is getting bigger and becoming more complicated,” says Belding. “Our model for delivering mobility services is allowing us to handle this kind of growth.”

Productivity

Cisco IT has performed three internal surveys of new mobile users. They were asked about how their mobile device has improved their work at Cisco. These surveys showed that on average the mobile device user gained about 15 minutes of productive time per day, by being able to access information when their laptops were unavailable and taking calls when they were away from their office phone or laptop Cisco Jabber client. People carry their smartphones almost all the time and can check their calendar or email, research issues, query tools, and respond to questions or issues whenever and wherever they like. This productivity gain of simply 15 minutes per day is estimated to have a value to Cisco of US$300 million per year.

Reduction of Service and Device Cost

Services and support costs are by far the highest portion of Cisco ITs budget for mobility, almost 10 times the cost of leasing the devices themselves. The BYOD program has provided opportunities to reduce services and support costs as well as device costs.

“During the economic downturn in 2009, we performed a complete audit of our mobile service expenses to identify where we could cut costs,” says Belding. “We were able to reduce our expenses by 30 percent simply by identifying lines that were no longer used and employees who didn't really need company-paid mobile devices given their job role.”

As more people prefer to bring their own device, Cisco-paid phones have dropped by two-thirds in the past two years, reducing Cisco IT’s overall spend on devices, managing their deployments, and break-fix support of mobile devices. Reducing the number of devices resulted in significant cost savings. Cisco IT saved about US$500,000 per year from that reduction. In addition, Cisco IT estimates (before the BYOD program) that increasing demand for more mobile devices would add another $850,000 per year in device upgrades, another cost avoidance for the BYOD program.

Cisco IT works hard to negotiate and reduce vendor costs, focusing on voice and data plan service providers to ensure that their discounted costs to Cisco continue to drop at the same speed that consumer mobile services do. Cisco IT also re-negotiates contracts with smartphone vendors supplying Cisco-owned phones, although employees are less and less interested in keeping those devices and prefer to buy their own.

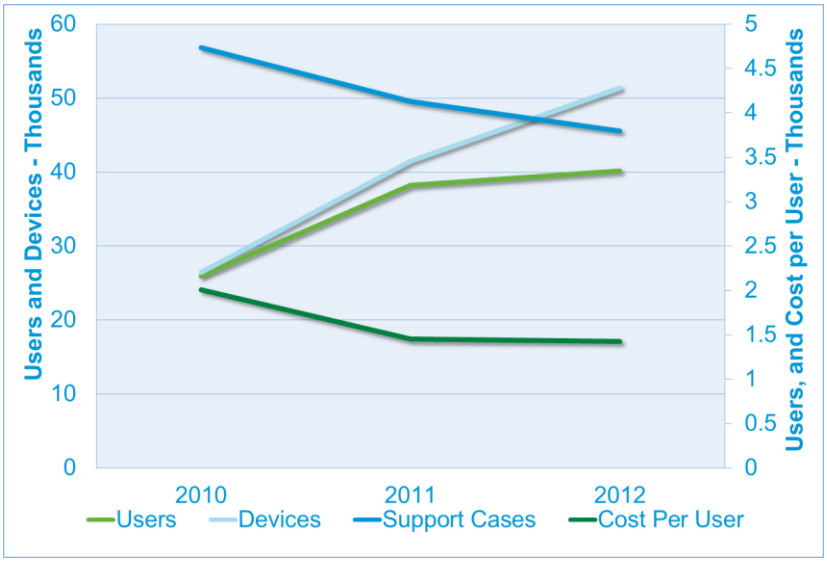
Reduction of Support Cost

The availability of online help resources for mobility services means the number of related support cases received by the Cisco helpdesk has declined steadily, with just 2.4 cases per 100 users per month as of early 2013. With the growing number of users and devices, 33 percent total of case reduction over the past 2 years was also a more impressive 40 percent per user case-load reduction, or a 56 percent per device case-load reduction (see Figure 6). Between 2011 and 2013:

- The number of mobile devices at Cisco rose 88 percent.
- The number of new mobile device users at Cisco rose 28 percent.
- The number of mobile service cases dropped 33 percent.
- User satisfaction increased 28 percent (as measured by user support surveys).

> "We were able to reduce our expenses by 30 percent simply by identifying lines that were no longer used and employees who didn't really need company-paid mobile devices given their job role."
> **– Brett Belding, Manager, Cisco IT Mobility Services**

Figure 6. User and Device Growth, Support Case and Cost per User Reduction Between 2010 and 2012



Lessons Learned

With more than a decade of experience in delivering mobility services to employees, Cisco IT has gained several

valuable lessons.

Secure BYOD access to the network without compromising user experience. Cisco IT realized very early that completing certain transactions and collaborating from a smartphone should be as easy as, if not easier than, doing the same from a laptop. For Cisco, this capability means using the native resources of the OS as often as possible and when it is necessary, creating an intermediary step, making it as transparent as possible.

For iPhone, Cisco employees must use the Cisco AnyConnect client that uses certificates to authenticate the user and encrypt and control data flow between the user and corporate data. AnyConnect was developed on the mobile client. Once validated and the certificates set up, AnyConnect will automatically launch and establish a secure connection whenever any tool (e.g., the browser, Cisco Jabber) is launched. This process takes an additional second or two and once connected, it remains connected (even during minor network drops) until the smartphone is turned off. Cisco IT is investigating the use of SSL rather than certificates to fulfill this function.

Educate users about Subscriber Identity Module (SIM) cards. Employees need to understand the limits of their BYOD service. Each phone needs to be identified and certified by Cisco IT before it can be connected to the network. Many trouble calls involve employees who buy a new phone, swap the SIM card from the old phone to the new phone to maintain mobile service information, and expect it to work. However, along with the need to provision Cisco IT services on the new phone, they must also be made aware of the differences in service plans and data usage required by the new phone vendor that may not be compatible with the old SIM card, especially if it is designed for use with a different carrier or device. These differences can affect the employee's mobile service charges and create unexpectedly high bills. To help prevent this issue, Cisco IT advises users not to swap SIM cards among phones.

Control costs with regular eligibility reviews. When Cisco pays for phone service, occasionally the service costs can be very high. This higher cost often comes from employees finding out that iPhone or Android phones typically use far more data than a Blackberry or discovering the true extent of roaming charges. Cisco IT offers employees tips for reducing their use of mobile phone minutes and the potential for overage charges. For example, Cisco IT recommends using the Cisco WebEx dial-back feature when participating in voice conferences from mobile phones. Using a local Wi-Fi service for data access can reduce roaming charges.

In addition, employees might not realize that using a smartphone as a portable Wi-Fi hotspot can mean costly extra charges. Employees with very high bills and their managers receive monthly feedback on costs from Cisco IT. Two additional procedures can help with cost control: reviewing an employee's continued eligibility when a corporate-paid account reaches its service renewal date, and requiring employees who change jobs within Cisco to reapply for mobile services approval from their new manager.

Plan for increasing user needs over time. The best service Cisco IT can provide employees one year becomes the foundation for a wider array of service requests the next year. In 2009, employees wanted iPhones to work as corporate devices in the same way that a limited set of corporate approved Blackberry and Nokia devices were allowed. In 2010, they wanted iPads and tablets to be supported and have intranet access to corporate services. In 2011, they wanted corporate applications supported on mobile devices such as Cisco WebEx Meeting Center and Cisco Jabber IM. In 2012, they wanted an application store filled with Cisco-specific mobile applications that would enable them to access current or new tools. And in 2013, they want access to secure cloud storage and other

external cloud services.

Also, as more employees brought multiple devices into work (laptop and one or more tablets or smartphones), Cisco IT found that some locations were running out of IP addresses. The network IT operations teams needed to increase the wireless IP address resource space in certain locations to cope with the expanding number of network-connected devices.

Mobility is a journey, not a destination, and a clear strategy and roadmap are critical to maximize return on investment and employee satisfaction.

As employees demand cloud services, provide secure cloud services. Cisco corporate policies on information security prohibit employees from forwarding or synchronizing confidential information in their business emails with an external file storage cloud service that allows viewing messages on a webpage. As these types of services become popular for personal use, employees might need specific warnings about the security risks. Cisco IT is leveraging the Cisco eStore to guide users to options that enable them to work easily and responsibly, and to provide them with secure tools that are as easy to use as less secure consumer cloud tools.

Provide resources for user self-support. It can be difficult for users to understand where to obtain support for network access and phone setup issues. For example, should they call the Cisco help desk, the mobile carrier, or a phone retailer? To encourage users to find support information themselves, Cisco IT continues to add content to the internal support service, making use of pages and posts, discussion forums, and click-to-call access to resources within the internal self-support community. In addition, Cisco IT improves the community by listening to complaints or problems, sometimes showing users how to access the information they need, and sometimes changing the interface to make the information more intuitive.

Develop policies and procedures for deleting device content. It is vital to manage sensitive information stored on a mobile device when an employee leaves the company. As part of the Rules of Use, Cisco requires employees to agree that their mobile device content will be wiped completely when their employment ends. Depending on the circumstances, Cisco IT may perform this wipe remotely or provide instructions for the employee to perform this task.

Next Steps

Cisco eStore

Cisco IT is developing the Cisco eStore, a single place where employees can conveniently find all the IT services and apps they need on any device (Figure 7). eStore will offer a range of services that include signing up for basic BYOD service, installing apps on smartphones or laptops, as well as installing IT services such as ordering a new laptop or home access service via Cisco Virtual Office (CVO). Cisco eStore provides a simplified, consistent user experience for Cisco workers to access their IT services and apps across multiple devices and platforms. Employees will no longer have to go to different places to configure their devices, because all services will be available directly from the eStore and provisioned automatically with very little input from the employee.

The eStore platform is Cisco IT's efficient new approach to a common ordering and provisioning framework, resulting in faster time to provision. Eventually, every Cisco IT solution will be available to employees. Cisco eStore is powered by Cisco Prime Service Catalog and Cisco Process Orchestrator.

Figure 7. Initial Vision of Cisco IT eStore

Broadening range of devices supported. Android is the next OS to be enabled as a secure device within the Cisco IT AnyDevice program. To date, its flexibility and the way that each service provider has customized Android OS to fit its own network and differentiate it from competitors has made Android an OS with many different personalities and many different security weaknesses to exploit. As employees start bringing in yet-to-be-announced devices, Cisco IT will address them.

Content virtualization in the cloud. Various cloud services offer content virtualization and work application platforms in the cloud. This model is very attractive to Cisco employees, who want to be able to access all their work resources from anywhere, on any device, safely and securely. Cisco IT is trialing two different sets of options: delivering internal private cloud solutions (e.g., Virtual Desktop Infrastructure, Virtualization Experience Infrastructure, cloud storage), and providing safe and secure cloud provider services under contract. In the end Cisco IT anticipates that in the long run HTML5 will be the protocol of choice for content and application virtualization.

BYOD is just one part of the broader mobility and consumerization of IT strategy. The goal is to enable any Cisco employee to have secure access to all corporate resources at any time, from any location, with any device.

For More Information

- Financial impact of BYOD in an enterprise
- Cisco solutions for mobility services
- Introduction to the Cisco BYOD Smart Solution
- For specific Cisco Validated Designs supporting mobility and BYOD
- For a Cisco Design Zone recorded webinar on BYOD

For information on securing a BYOD environment using the Cisco Identity Services Engine, see: http://www.cisco.com/en/US/prod/collateral/vpndevc/ps5712/ps11637/ps11195/qa_c67-703415.html.

- Cisco on Cisco blog contains posts on mobile communications topics

To read additional Cisco IT case studies on a variety of business solutions, visit Cisco on Cisco: Inside Cisco IT.

Note

This publication describes how Cisco has benefited from the deployment of its own products. Many factors may have contributed to the results and benefits described; Cisco does not guarantee comparable results elsewhere.

Some jurisdictions do not allow disclaimer of express or implied warranties, therefore this disclaimer may not apply to you.

CISCO PROVIDES THIS PUBLICATION AS IS WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING THE IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **www.cisco.com/go/offices.**