Cisco Bring Your Own Device

Device Freedom Without Compromising the IT Network

Last Updated: July 17, 2012

About the Authors

Neil Anderson

Neil Anderson, Director of Systems Architecture, Systems Development Unit (SDU), Cisco Systems

Neil is the Director of Systems Architecture with Cisco and has been leading systems development at Cisco for over 10 years. He has more than 25 years of broad systems experience, including public telephone networks, mobile phone systems, and IP networks. At Cisco, Neil's focus is on Enterprise network architecture including routing, switching, wireless and mobility, security, video, and emerging technologies. Neil is also the coauthor of five books in the Networking Simplified series published by Cisco Press

.

ALL DESIGNS, SPECIFICATIONS, STATEMENTS, INFORMATION, AND RECOMMENDATIONS (COLLECTIVELY, "DESIGNS") IN THIS MANUAL ARE PRESENTED "AS IS," WITH ALL FAULTS. CISCO AND ITS SUPPLIERS DISCLAIM ALL WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE. IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THE DESIGNS, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

THE DESIGNS ARE SUBJECT TO CHANGE WITHOUT NOTICE. USERS ARE SOLELY RESPONSIBLE FOR THEIR APPLICATION OF THE DESIGNS. THE DESIGNS DO NOT CONSTITUTE THE TECHNICAL OR OTHER PROFESSIONAL ADVICE OF CISCO, ITS SUPPLIERS OR PARTNERS. USERS SHOULD CONSULT THEIR OWN TECHNICAL ADVISORS BEFORE IMPLEMENTING THE DESIGNS. RESULTS MAY VARY DEPENDING ON FACTORS NOT TESTED BY CISCO.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

Cisco Bring Your Own Device

Cisco Bring Your Own Device

Introduction

Bring Your Own Device (BYOD) has become one of the most influential trends that has or will touch each and every IT organization. The term has come to define a megatrend occurring in IT that requires sweeping changes to the way devices are used in the workplace.

What is BYOD? Does it mean employees pay for their own devices they use for work? Possibly, but the BYOD trend means much more. It is about end users being able to use the compute and communication devices they choose to increase productivity and mobility. These can be devices purchased by the employer, purchased by the employee, or both. BYOD means any device, with any ownership, used anywhere.

This paper discusses the how this trend will affect businesses, explores the challenges it creates for IT, and outlines the Cisco® technologies that are part of the solution. Cisco offers a comprehensive architecture to address these challenges, allowing end users the freedom to bring their choice of device to work while still affording IT the controls to ensure security and prevent data loss.

Business Drivers

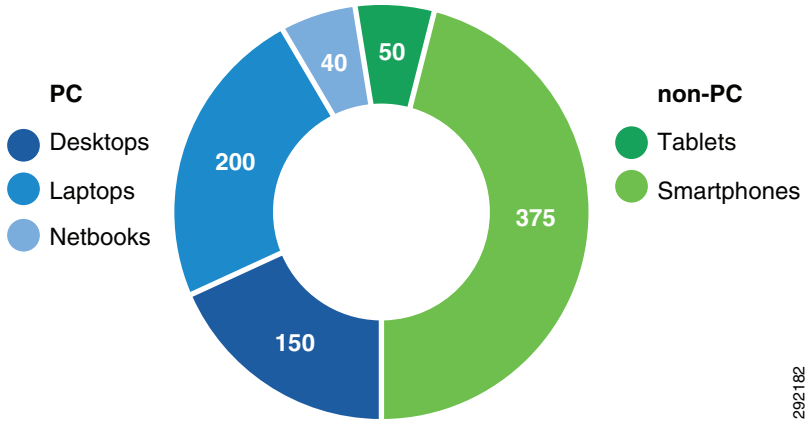
To understand the challenges BYOD poses, it is helpful to understand the business trends that are driving BYOD adoption.

Consumer Devices

Previously, employers provided desktop and laptop computers that were typically the most advanced tools to which an employee had access. With the explosion in consumer devices, including laptops, netbooks, tablets, smartphones, e-readers, and others, employees typically have some of the most advanced productivity tools being used in their personal lives. Employees quickly asked their IT organizations: Why can't I use these tremendous productivity tools at work? Many IT organizations initially rejected the idea, citing security reasons and the inability to scale to approve and support more than a small handful of devices.

Corporate Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

Figure 1 PC and Non-PC Sales, 2011 (Millions)—Source: Deloitte, 2011



In the last year, the persistence of end-users demanding to leverage their tablet computers and smartphones to extend their productivity, even if they had to purchase the devices themselves, has led many IT departments to adopt less restrictive policies, allowing employees basic connectivity or, increasingly, full access to the IT network and corporate applications. This trend is likely irreversible and every IT organization will need to quickly adapt to the consumer device phenomenon.

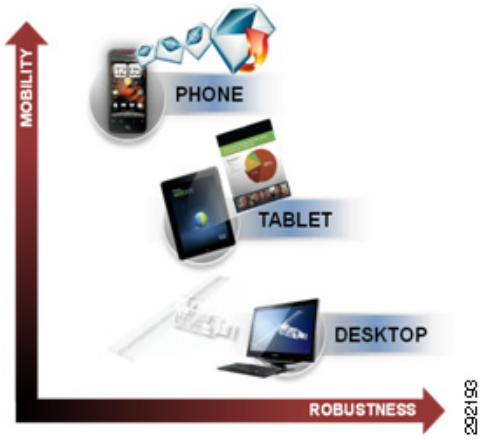
Multiple Needs and Multiple Devices

Many people had a desktop PC or laptop and added a mobile phone for voice calls. Mobile phones have largely been replaced with smartphones that can run applications and include Internet access and a camera. Many smartphones and tablets are as powerful and capable as laptops and PCs, enabling a new class of uses and applications

There is speculation that in the future a single device will be used for all needs: computing, communications, and applications.

However today most believe there will continue to be different devices best suited to particular uses. For example, a laptop is not as portable as a smartphone, so people are likely to carry their smartphone for mobile communications. Tablets are powerful devices as well, but it is likely laptops and PCs will still be used for document creation and publishing. This means people will more likely carry and use multiple devices and less likely that a single, all-purpose device will emerge.

Figure 2 Variety of Devices



The impact of this trend is that many more devices will be connected to the network by the same employee or person, often simultaneously, and likely lead to a large increase in overall connected devices.

Work and Personal Overlap

Increasingly, work is an activity that people do, not a place to which they go. Extended connectivity through mobile and remote access to the corporate network gives employees tremendous flexibility and increased productivity. It also leads to a blurring of the line between work time and personal time, with employees trading set work schedules for the flexibility of working when and where they want to, often interweaving work and personal tasks.

A side effect of this flexibility is that users probably do not want to carry and switch between personal and work devices. Most employees want to be able to use a single smartphone, tablet, or laptop for both work and personal tasks and not also carry around corporate devices.

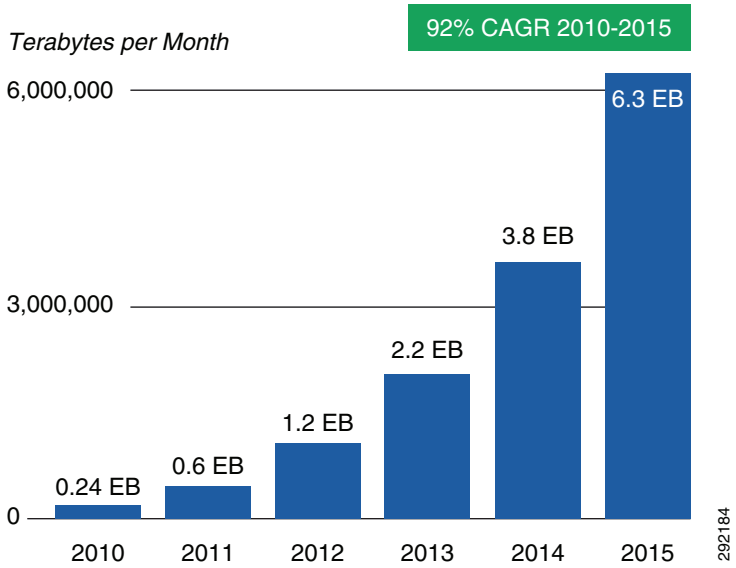
Device ownership is not clear cut. Many employees are willing to use their personal tablet or smartphone, for example, to access work applications. Many employers are considering or have implemented subsidy programs, whereby an employee is provided with money for devices, but it is up to the employee to purchase the devices they want.

The effect of this time and device overlap is that corporate and personal data will be increasingly co-mingled on devices, leading to security and privacy challenges.

Anywhere, Anytime Mobility

It is estimated that mobile devices and the traffic they create on networks will increase by 26X between 2010 and 2015, driven by more powerful smartphones and tablets, with users demanding Internet access and access to applications wherever and whenever they want. Enabling this is an explosive build-out of WiFi networks by employers, 3G and 4G networks by mobile providers, as well as public WiFi by retailers, municipalities, etc.

Figure 3 *Worldwide Mobile Data Forecast 2010-2015 (Source: Cisco Visual Networking Index, 2011)*



The more employees can easily access work using WiFi and mobile networks, the more widespread these networks will become, thereby further enabling access. The end result is pervasive connectivity anywhere and anytime, which means corporate networks will have more devices connected more frequently, leading to an even broader need for the 24/7 availability of applications.

Video, Collaboration, and Rich Media Applications

Work and personal communications both increasingly use rich media, driving a large increase in the amount of video and multimedia traffic traversing the network. Collaboration applications and pervasive mobility will continue to increase the use of rich media.

As employees use collaborative applications and adopt mobile work styles, the demands on mobile and WiFi infrastructures will be pronounced. Another driver of this trend are the capabilities being integrated into more powerful consumer devices, commonly found with high-definiton (HD) cameras and video. As bandwidth and available 4G and WiFi services increase, applications transmitting HD media streams will be common.

The experience on many tablets and smartphones is typically best effort today, but expect this to reach production quality in the future. Communications and collaboration devices like the Cisco Cius™ will further drive the need for seamless mobile HD video and collaboration.

Challenges for IT Organizations

Adopting BYOD comes with a set of challenges for the IT organization. Many of the benefits of BYOD, such as having the choice of any device and anywhere, anytime access, are somewhat antithetical to traditional IT requirements for security and support.

Providing Device Choice and Support

Traditionally, IT pre-determined a list of approved workplace devices, typically a standardized desktop, laptop, and perhaps even a small, standardized set of mobile phones and smartphones. Employees could choose among these devices, but generally were not permitted to stray from the approved devices list.

With BYOD, IT must approach the problem differently. Devices are evolving so rapidly that it is impractical to pre-approve each and every device brand and form-factor. It is also somewhat impractical to expect IT organizations to have the same level of support for each and every device that employees may bring to the workplace.

Hence most IT organizations have to establish, at a macro level, what types of devices they will permit to access the network, perhaps excluding a category or brand due to unacceptable security readiness or other factors. Support must also be considered, such as adopting more IT-assisted and self-support models.

Maintaining Secure Access to the Corporate Network

Device choice does not mean sacrificing security. IT must establish the minimum security baseline that any device must meet to be used on the corporate network, including WiFi security, VPN access, and perhaps add-on software to protect against malware.

In addition, due to the wide range of devices, it is critical to be able to identify each device connecting to the network and authenticate both the device and the person using it.

On-Boarding of New Devices

Most BYOD implementations will have a wide-range of devices including desktop PCs, laptops, netbooks, smartphones, tablets, e-readers, and collaboration devices like the Cisco Cius. It is likely some devices will be corporate owned and managed, while other devices may be employee purchased and self-supported.

On-boarding of new devices—bringing a new device onto the network for the first time—should be simple and, ideally, self-service with minimal IT intervention, especially for employee bought devices. IT also needs the ability to push updates to on-boarded devices as required.

Ideally on-boarding should be clientless, meaning no pre-installed software is required. This has an added benefit: if a self-service on-boarding model is successfully implemented, it can be easily extended to provide access to guests as well.

Enforcing Company Usage Policies

Businesses have a wide range of policies they need to implement, depending upon their industry and its regulations and the company's own explicit policies. Adoption of BYOD must provide a way to enforce policies, which can be more challenging on consumer devices like tablets and smartphones.

Another complication results from the mixing of personal and work tasks on the same device. Smartphones are likely used for business and personal calls and tablets likely have both personal and business applications installed. Access to the Internet, peer-to-peer file sharing, and application use may be subject to different policies when a user is on their personal time and network and when they are accessing the corporate network during work hours.

Visibility of Devices on the Network

Traditionally an employee had a single desktop PC or laptop on the network and probably an IP desk phone. If the employee called IT for support, it was likely straightforward to locate that user's device on the network and troubleshoot the issue.

With BYOD adoption, each employee is likely to have three, four, or more devices connected to the network simultaneously. Many of the devices will have multiple modes, able to transition from wired Ethernet to WiFi to 3G/4G mobile networks, moving in and out of these different connectivity modes during a session. It is critical for IT to have tools that provide visibility of all the devices on the corporate network and beyond.

Protecting Data and Loss Prevention

One of the largest challenges with any BYOD implementation is ensuring protection of corporate data. If a corporate asset, such as a laptop, is used to access business applications and data, typically that asset is tightly controlled by IT and likely subject to more restrictive usage policies.

Some industries need to comply with confidentiality regulations like HIPAA, security compliance regulations like PCI, or more general security practice regulations like Sarbanes-Oxley and others. Companies need to show compliance is possible with BYOD adoption, which can be more challenging than with a corporate-owned and managed device.

An employee-owned tablet or smartphone is likely being routinely used for personal access and business applications. Cloud-based file sharing and storage services are convenient for personal data, but can be potential sources of leakage for confidential corporate data.

IT must have a strategy for protecting business data on all devices whether corporate managed or employee self-supported and managed. This may include a secure business partition on the device which acts as a container of corporate data that can be tightly controlled and may also include the need for a Virtual Desktop Infrastructure (VDI) application to allow access to sensitive or confidential data without storing the data on the device.

Revoking Access

At some point in the lifecycle of a device or employee, it may become necessary to terminate access to the device. This could be due to a lost or stolen device, an employee termination, or even an employee changing roles within the company.

IT needs the ability to quickly revoke access granted to any device and possibly remotely wipe some or all of the data (and applications) on the device.

Potential for New Attack Vectors

Because the devices accessing the corporate network have wide-ranging capabilities and IT may not be able to fully evaluate, qualify, and approve each and every device, there is the potential for new security attack vectors to be opened.

For example, many tablets have the capability to enable an ad hoc WLAN. If an authenticated device has other devices tethered to it through an ad hoc WLAN, it may be possible for non-authenticated devices and users to gain access to the corporate network by connecting through the authenticated device. The same is true when tethering a laptop over Bluetooth through a smartphone.

The challenge for IT is how to permit the growing number of devices and capabilities to be used, while still maintaining the control to enforce policies, such as automatically disabling an ad hoc WLAN function on an authorized connected device.

Ensuring Wireless LAN Performance and Reliability

As wireless access becomes pervasive, performance and reliability expectations are the same as what is expected from the wired network, including reliable connectivity, throughput, application response times, and increasingly voice, video and other real-time collaboration applications.

This fundamental shift demands that IT change the service level of the corporate WLAN network from one of convenience to a mission critical business network, analogous to the wired network. Design and operation of the WLAN must include high availability, performance monitoring and mitigation, as well as seamless roaming.

Managing the Increase in Connected Devices

The increasing number of devices connected to the network, most likely with each employee having many devices simultaneously connected, can lead to IP address starvation as most legacy IP address plans were created under the assumption of fewer devices. This may hasten the need for IPv6 deployments both at the Internet edge as well as inside the enterprise network.

Challenges for End Users

The demand for BYOD is largely driven by users who want to choose the devices they use in the workplace. From a user perspective, there are challenges to address.

Keeping it Simple

BYOD solutions and technologies are quickly evolving, however one of the largest challenges is how to make it simple for people to get connected to and use corporate resources. The number of device possibilities, the range of connection types and locations, and the lack of widely adopted approaches can translate to difficulties for users.

Each device brand and form factor may require slightly different steps to be on-boarded and connected. Security precautions and steps may also vary depending upon how and where the user is trying to connect. For example, the corporate WiFi may require credentials, whereas connecting through a public WiFi hotspot may require credentials, a virtual private network (VPN), and other security steps.

Ultimately any BYOD solution needs to be as simple as possible for users, provide a common experience no matter where and when they are connecting, and be as similar as possible across devices.

Mixing Personal Device With Work

BYOD brings a mix of personal and work tasks on the same device. Contact lists, E-mail, data files, applications, and Internet access can pose challenges. Ideally, users want to separate their personal data and activities from work. Personal photos, text messages, phone calls, and Internet browsing performed

on their own time needs to be subject to personal privacy, while documents, files, applications using corporate data, and Internet browsing performed on company time needs to be in compliance with corporate policies.

Some employers make connecting with an employee-owned device contingent on signing an agreement so the company can monitor compliance, acceptable use policies, and otherwise act to protect corporate data. In some cases this may include remote wiping of all data on the device—potentially including personal data—which obviously can be a source of contention between IT and users if not properly managed.

Getting the Productivity and Experience Needed

As discussed earlier, one of the major drivers of BYOD is employees who want to take advantage of productivity tools they use as consumers in the workplace. Companies want to embrace and benefit from that productivity, but also need to apply the appropriate security and policies to protect corporate data.

If such security measures are too intrusive, they could erase any productivity gains. For example, a common complaint is that companies that lock down access to business applications and data through the deployment of VDI clients on a tablet device degrade the user experience to the point where an employee does not get a tablet experience. VDI clients are likely to improve, including user experience, as deployments of tablets and smartphones continue to grow.

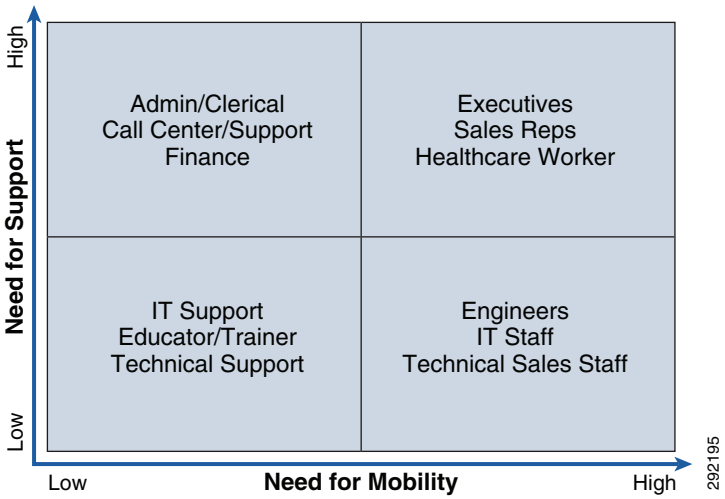
Considerations for BYOD Adoption

For any widespread adoption of BYOD, there are a number of considerations that need to be thought about beforehand.

Understand User Segments and Needs

It is important to understand that there are different segments of users within any BYOD implementation. One recommendation is to conduct a user segmentation analysis within the company to help understand needs and likely level of required support. An example is shown in Figure 4.

Figure 4 User Segments and Needs



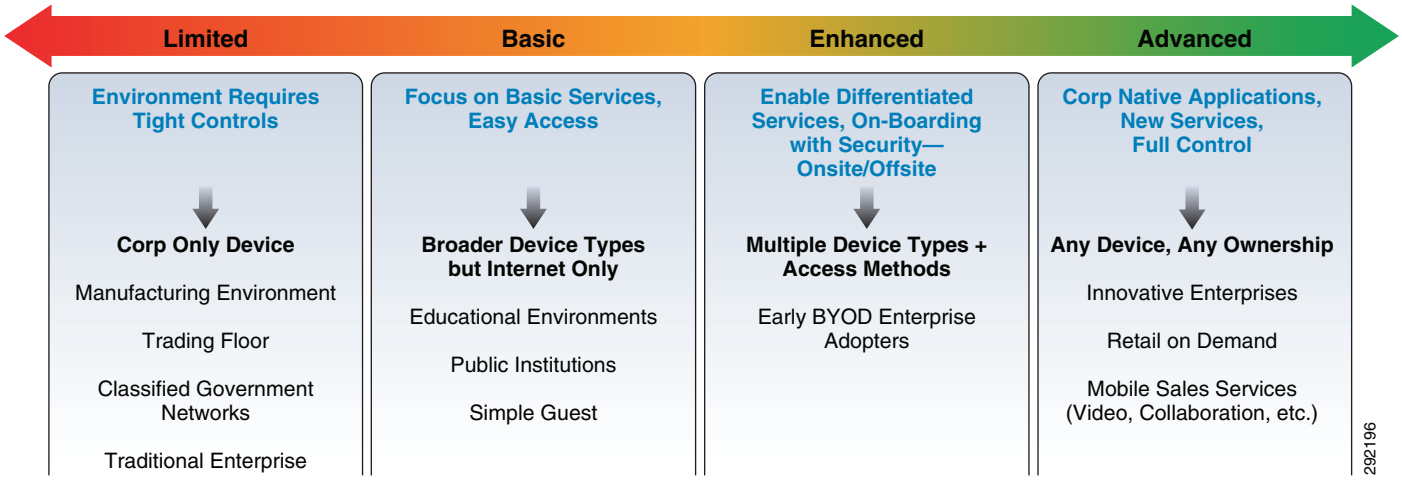
Every company is different. Figure 4 evaluates employee roles against the need for mobility and mobile applications and against the likely level of required support. BYOD deployments are easy with users who only need low levels of IT support, possibly using self-support communities to share best practices. Deployments may be more difficult with users who have high mobility needs but also require high support levels, such as executives.

Conducting such an analysis will help understand entitlement policies and support models and may prevent frustration and cost overruns in the IT budget.

Deciding on a BYOD Adoption Strategy

Different businesses will approach BYOD with different expectations across a spectrum of adoption scenarios. Every business needs a BYOD strategy, even if the intention is to deny all devices except IT approved and managed devices. Figure 5 shows a number of possible adoption scenarios into which most businesses fit.

Figure 5 BYOD Adoption Scenarios



Businesses within industries with high degrees of regulation, such as finance or secure government agencies, may need to take a restrictive approach with BYOD adoption to protect sensitive data. Devices may need to be tightly controlled and managed as in the traditional IT approach, which may still be valid in these instances.

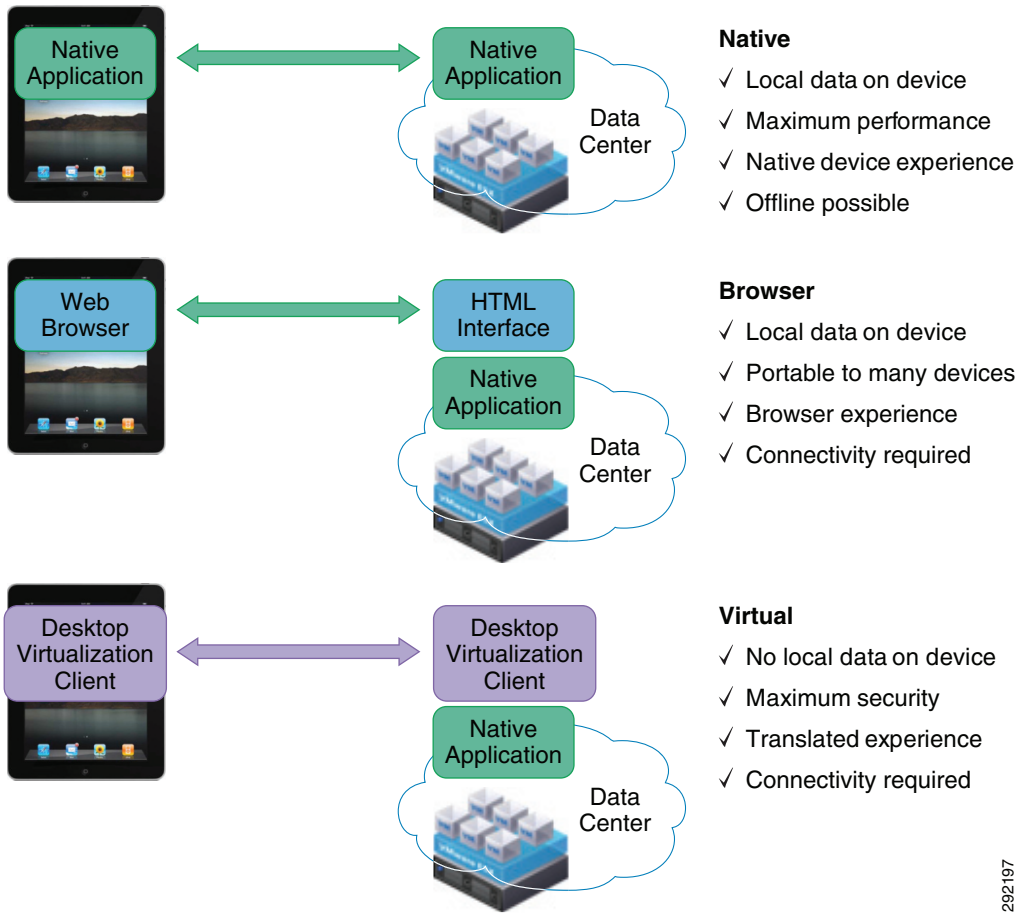
For many companies, adoption will range from allowing a broader set of devices with restrictive access to applications to embracing BYOD in full, encouraging broad adoption of many or all device types and deploying security measures to enable access to a broad set of enterprise applications and data. In the broadest sense, some companies will adopt a "mobile first" strategy, whereby their own internal applications development will be prioritized on tablets and smartphones, seeking competitive advantage by leveraging the broadest set of productivity tools and devices.

Understanding where your business will fit now and in the future along the adoption spectrum is useful to prepare for security policies, entitlement, and overall strategy for the BYOD initiative.

Considering Application Strategies

Securing and preventing the loss of corporate data is a top concern when implementing BYOD. It is important to understand three possible application architectures and the trade-offs involved: native, browser, and virtual. These are shown in Figure 6.

Figure 6 Native, Browser, and Virtual Modes



In native mode, applications running on the device communicate directly with the application server in the host data center (or cloud). Data may be exchanged and stored directly on the BYOD device. Typically the application performance and user experience are closest to the specific device; in other words, a business application functions much like any other application on the device. All the productivity benefits and device behavior are preserved and applications can be tailored to provide enhanced experiences.

A browser approach is increasingly being adopted for application access due to the ease of portability across devices and operating systems. Essentially any device with a standard HTML browser capability can be used to access the application. The disadvantages are that much like native mode, data may be exchanged and stored directly on the BYOD device, leading to security challenges and concerns about data loss. In addition, there may be some sacrifice of user experience.

To contrast, in virtual mode applications exist on the application server in the data center (or cloud) and are represented through a VDI client on the device. Data is not stored locally on the BYOD device. Only display information is exchanged and rendered on the BYOD device. While this method provides maximum data security, user experience may be a compromise due to the translation from an application server to the form-factor and OS native to the BYOD device. Early adopters of this approach have provided somewhat negative feedback.

It is important to make decisions about which mode, native or virtual, will be relied on for the application architecture. Many companies may use a hybrid approach, using native mode for many standard business applications and virtual mode for a subset of applications with stricter confidentiality or sensitive data requirements.

Extending Collaboration to BYOD Devices

Ultimately, people want to connect to the network not only for access to data applications, but also to collaborate with one another. Just as in traditional workspaces, users with BYOD devices want access to their company's voice, video, and conferencing services.

Standalone approaches, such as relying on the smartphone's cellular communications, can be somewhat effective. To be truly effective, it is essential to have an integrated approach that makes people easily reachable within their company's communications directory and systems. Another consideration is how then do we extend these services to devices without cellular voice capabilities, such as an Apple iPad?

A complete BYOD solution must consider how to extend the full suite of collaboration applications to BYOD devices, including integrated voice, video, IM, conferencing, application sharing, and presence. Any solution needs to consider not only the employees using BYOD devices, but also others trying to collaborate with them.

Have an Encompassing End User Agreement

Although not part of the network architecture, one area that must be well thought out prior to any BYOD implementation is the end user agreement (EUA). Because of the mixing of personal and corporate data, and the potential of having employee-owned devices being used for work, it is critical to outline policies up front and be sure to communicate these to employees in advance.

IT organizations need to familiarize themselves with laws, including the Computer Fraud and Abuse Act, the Wiretap Act, and Communications Assistance for Law Enforcement Act (CALEA).

What will company policies be? Will communications be subject to monitoring? Will policies apply to both corporate and personal? Areas to be addressed include (but are not limited to):

- Text messaging

- Voice calling
- Internet browsing
- Instant messaging
- E-mail
- GPS and geo-location information
- Applications purchased/installed
- Stored photographs and videos
- Device “wiping”

As a simple example, many businesses regularly filter and monitor Internet access to ensure compliance with policies against accessing inappropriate Web sites at work. Most BYOD devices have direct internet access through public WiFi and/or 3G/4G mobile Internet access. It would be common to have a policy against browsing X-rated Web sites on a device connected through the corporate network. Will the same policy apply if the employee decides to browse sites on their employee-owned device, on personal time, through public Internet access?

As another example, it would be common to have policies against transmitting inappropriate E-mails containing very personal photos through E-mail or text messaging while using a corporate-owned device or corporate network. Will the same policies apply to personal E-mails or personal text messaging on an employee-owned device? Which communications will be monitored? Which will not?

There have been several legal challenges recently for cases involving an employer who remotely “wiped” an employee-owned device, including both the corporate and personal data it contained. Imagine the surprise as an employee when by using your new tablet to access the corporate network, you unknowingly agreed to let IT delete your favorite family photos. Other challenges exist around potentially illegal wiretap situations where employees are challenging that their text message conversations were being illegally monitored by their company who failed to notify them.

The key to avoiding legal liabilities is to notify, notify, and notify again. Make it clear to employees in a written policy that they must accept how the company will treat corporate and personal data and communications on the BYOD device. By agreeing to the EUA, make it clear what rights the employee is forfeiting to gain access to the network with an employee-owned device.

Have a Lost or Stolen Device Policy

Similar to the previous discussion about having a complete EUA in place, businesses should have a plan in place for how lost or stolen devices will be handled. What will be the process for notification by employees? What are the necessary steps to remove access to the corporate network? What steps can and will be taken to remotely remove local data stored on the device?

Different solutions offered in the market provide varying degrees of capabilities to reach out to a device remotely and destroy data or applications to insure they remain confidential. Consider the types of data that are likely to be stored on BYOD devices and integrate mitigation plans into the overall BYOD strategy before deployment.

Cisco BYOD Architecture

Cisco provides a comprehensive BYOD solution architecture, combining elements across the network for a unified approach to secure device access, visibility, and policy control. To solve the many challenges described earlier, a BYOD implementation is not a single product, but must be integrated into the intelligent network.

The Cisco BYOD solution builds on the Cisco Borderless Network architecture and assumes best practices are followed in network infrastructure designs for campus, branch offices, Internet edge, and home office implementations.

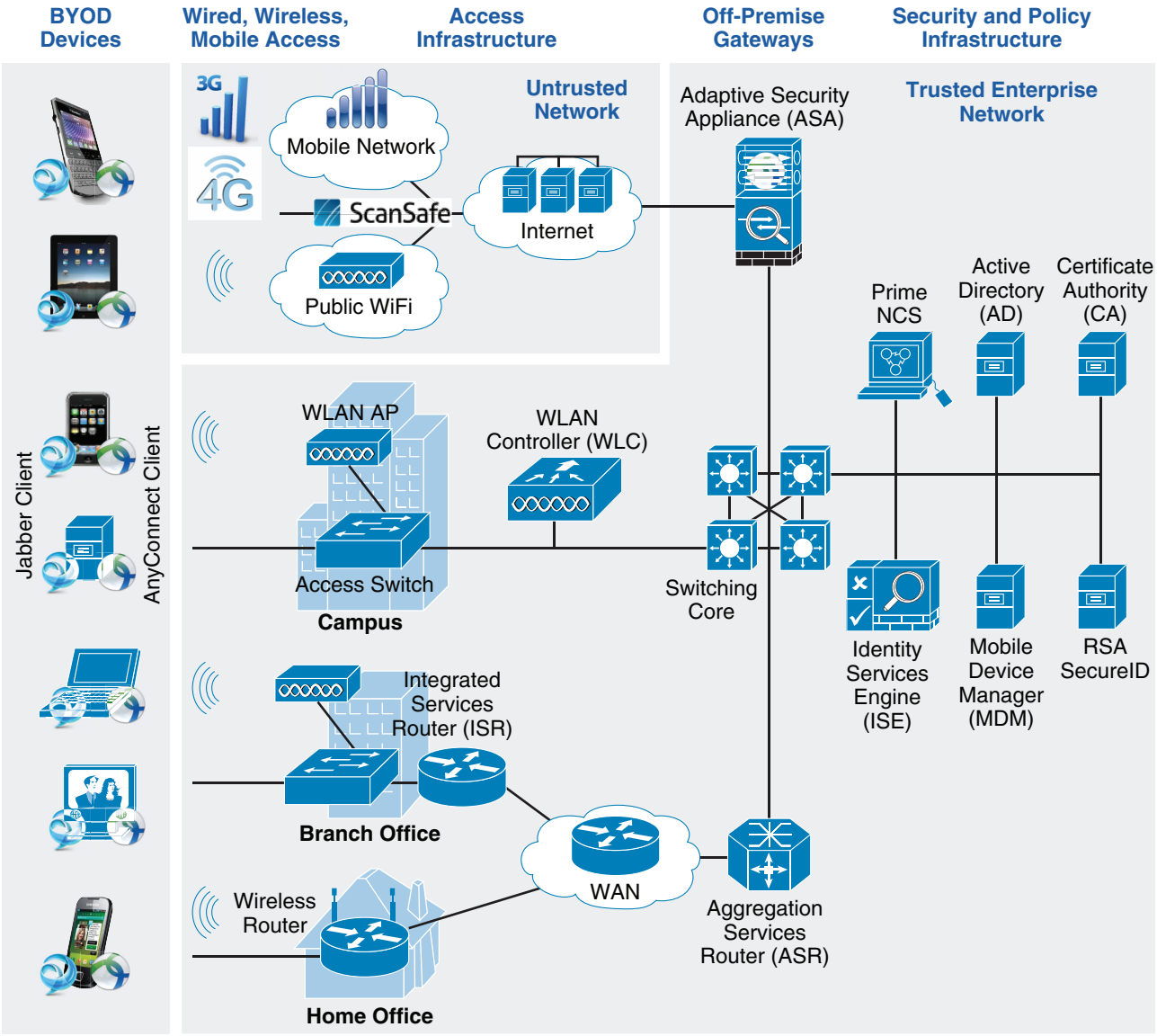
High-Level Solution Architecture

A comprehensive BYOD solution must provide for wired, WiFi, remote, and mobile access to the network, must be supported across many device types and brands, and must be capable of enforcing the various policies across the spectrum of businesses and industries. In addition, as devices move from one context to another, for example from the corporate WiFi network to a public 3G/4G mobile network, the BYOD solution must be able to provide secure access while keeping the experience seamless for the user.

It is critical to any BYOD strategy to consider comprehensive access to the corporate network, which means not only the corporate WLAN, but also wired access in major campuses, wired and wireless access in branch and home offices, as well as remote access over the Internet, mobile 3G/4G, and public WiFi hotspots. Any design that does not consider the broad range of possible network access contexts will fall short of providing a manageable and scalable solution for IT.

Figure 7 shows the high-level solution architecture and major components of the Cisco BYOD solution.

Figure 7 HIgh-Level BYOD Solution Architecture



Cisco Solution Components

The sections which follow outline the various Cisco components of the solution architecture and the role they perform.

Cisco Catalyst Switches

Cisco Catalyst® switches, including the Catalyst 3000, Catalyst 4000, and Catalyst 6000 families, provide wired access to the network and handle authentication requests to the network with 802.1x. In addition, access switches provide power-over-Ethernet (PoE) for devices needing power, including VDI workstations, IP phones, and WLAN access points (APs).

Cisco Integrated Services Routers

Cisco Integrated Services Routers (ISR), including the ISR 1900, ISR 2900, and ISR 3900, provide WAN connectivity for branch and home offices and connectivity for the wired and WLAN infrastructure in the branch office. In addition, ISRs may provide direct connectivity to the Internet and cloud services, application and WAN optimization services, and may also serve as termination points for VPN connections by mobile devices.

With the Secure Device Provisioning (SDP) function in the ISR, it is also possible to serve as the Certificate Authority (CA), which is useful for relatively smaller implementations.

Cisco Wireless LAN Access Points

Cisco Wireless LAN (WLAN) APs, including the AP3500 and AP3600, provide WiFi connectivity for the corporate network and handle authentication requests to the network via 802.1x. In addition, the WLAN provides critical functions for reliable, high performance mobile device connectivity.

Cisco Wireless LAN Controller

Cisco Wireless LAN Controller (WLC) is used to automate wireless configuration and management functions and to provide the visibility and control of the WLAN. The WLC is able to interact with the Identity Services Engine (ISE) to enforce authentication and authorization policies across device endpoints.

Cisco Adaptive Security Appliance

Cisco Adaptive Security Appliance (ASA) provides traditional edge security functions, including firewall and Intrusion Prevention System (IPS), as well as providing the critical secure VPN (AnyConnect) termination point for mobile devices connecting over the Internet, including public WiFi hotspots and 3G/4G mobile networks.

Cisco AnyConnect Client

Cisco AnyConnect™ client provides 802.1x supplicant capability on trusted networks and VPN connectivity for devices that access the corporate network from un-trusted networks, including public Internet, public WiFi hotspots, and 3G/4G mobile networks. Deploying and managing a single supplicant client has operational advantages as well as provides a common look, feel, and procedure for users.

In addition, the AnyConnect client can be leveraged to provide device posture assessment of the BYOD device, as well as a degree of policy enforcement and enforcing usage policies.

Cisco Identity Services Engine

Cisco Identity Services Engine (ISE) is a core component of the Cisco BYOD solution architecture and provides a number of services including:

- Self-service registration and enrollment portals
- Authentication
- Authorization
- Device profiling

- Device registration and provisioning
- Certificate enrollment
- Posture assessment
- Policy definition
- Interface to identity stores (e.g., Active Directory® [AD])
- Reporting and blacklisting of lost or stolen devices

One of the most important functions Cisco ISE provides is the ability to have a single location for registration of devices. When devices first connect to the network, they can be redirected to a self-service (or IT intervention) registration portal where users can register the device, enroll the device, and receive auto-provisioning pushed to the device. This is an essential service for lowering the burden on IT to have to touch and pre-provision every device on the network and also gives IT the visibility to devices accessing the network.

In addition to core functions such as authentication and authorization, Cisco ISE provides intelligence about devices connecting to the network through device profiling. Device profiling can be used for discovering, locating, and determining the type and capabilities of endpoints that attach to the network to deny or enforce specific authorization rules.

For example, the combination of device profiling, posture assessment, and policy enforcement can be used to enforce BYOD policies such as:

- Allow employee-owned iPads® access to the network, but only HTTP traffic
- Deny iPhones® access to the network if they have been jail broken
- If the Android™ device is corporate owned, grant full access

Cisco Prime

Cisco Prime™ provides network management and control functions, including key user and device visibility, as well as network device provisioning.

Cisco ScanSafe Cloud Web Security

Cisco ScanSafe extends the security capabilities most enterprise customers have on-premise through a cloud-based solution to protect BYOD clients when they are off-premise. By directing BYOD clients to access the internet through the ScanSafe cloud, security scanning is performed to filter Web access, detect malware, discover anomalous behavior, and provide real-time feedback to companies. Extending BYOD device protection is essential when the device leaves the enterprise network to prevent compromise and potential security attack vectors when the device rejoins the on-premise enterprise network.

Cisco Jabber

Cisco Jabber extends collaboration to BYOD devices by integrating the device into the Unified Communications suite of products. Users can easily use voice and video communications, access voice messages, and communicate through IM. Jabber clients also participate in Presence as well as having access to the same conferencing and desktop sharing applications as more traditional employee computers, including Cisco WebEx.

Figure 8 Cisco Jabber on Apple iPad

Third-Party Solution Components

The sections which follow outline the various third-party (non-Cisco) components of the solution architecture and the role they perform.

RSA SecurID

The RSA SecurID tokens and Authentication Server are used to provide two-factor (secret PIN and one-time password code) authentication for strong security when connecting through a VPN.

Mobile Device Manager

The Mobile Device Manager (MDM) provides centralized endpoint management for multiple BYOD device operating systems. Functionality and support varies across different MDM vendors, however typical functionality includes device configuration, on-device encryption, password enforcement, and self-service provisioning.

In addition to the network access-facing functions above, the MDM can also serve as an important security service on the end device providing authentication services for applications.

The Cisco BYOD solution architecture can work with a number of MDM offerings as an optional component.

Certificate Authority

The Certificate Authority (CA) is used to issue digital certificates to devices to establish trust for network access using a Public Key Infrastructure (PKI) implementation. A number of standard CA implementations can be used as part of the BYOD solution. For the purposes of this paper, the solution was validated with two types of CA: Microsoft® CA Services and Cisco IOS Secure Device Provisioning (SDP) hosted on an ISR (see Cisco Integrated Services Routers).

Microsoft Active Directory

The Microsoft Active Directory (AD) provides a central database of identities and groups and is commonly used by many businesses for centralized identity management. Rather than duplicating an identity store, the Cisco BYOD solution architecture was validated using AD as the external identity store for the Cisco ISE.

Supported Devices

The Cisco BYOD solution supports a wide range of devices, although capabilities and functionality varies depending upon the device or operating system. Consult detailed design guidance for specific functionality and limitations by device type. Table 1 shows the current device types validated with the solution.

Table 1 Supported Devices

Device	Wired	Corp WiFi	Public WiFi	3G/4G Mobile
Android smartphones and tablets[1]		Yes	Yes	Yes
Apple® OS X® Mac®	Yes	Yes	Yes	
Apple iOS™ iPhone		Yes	Yes	Yes
Apple iOS iPad/iPad2		Yes	Yes	Yes
Cisco Cius (Android)	Yes	Yes	Yes	Yes
Samsung™ Galaxy™ (Android)		Yes	Yes	Yes
Microsoft Windows® XP PC	Yes	Yes	Yes	
Microsoft Windows 7 laptop	Yes	Yes	Yes	

1. Android device support dependent upon OS version and support.

Generally, device support is a function of support level of Cisco AnyConnect and the Mobile Device Manager (MDM) being used. Most devices that can securely connect to WiFi can participate.

Key Advantages of the Cisco BYOD Solution

The Cisco BYOD solution integrates the Cisco products, third-party products, and devices discussed previously into a comprehensive BYOD approach which is tightly integrated across the network infrastructure. This offers a unique set of advantages over other solutions.

Secure Access for Any Device

Through a combination of X.509 digital certificates, two-factor authentication, Cisco AnyConnect client, and 802.1x, a wide variety of devices can be supported with secure access to the network.

Self-Service On-Boarding

The integrated approach allows for devices to be self-enrolled the first time they connect to the network. Each device is fingerprinted so it can be identified upon returning for subsequent network access attempts.

Centralized Enforcement of Company Usage Policies

Cisco Identity Services Engine (ISE) provides a centralized single source of policy across the organization that can be enforced across different network access types.

Differentiated Access and Services

The Cisco BYOD solution provides a means to identify devices and users and provides differentiated services based on custom policy options. For example, employees using corporate-owned and managed devices can be treated differently than employees using their own unmanaged devices at work. Similarly, contract employees, partners, guests, customers, students, and other classifications that are important to the business or entity can be identified and treated according to the business policies, restricting access to only the set of services and access to which they are entitled.

High Performance and Reliable Wireless LAN

The Cisco BYOD solution includes industry leading WLAN technologies to enable the best possible performance and reliability for wireless clients. Technologies including Cisco CleanAir™, ClientLink, and 4x4 antenna design fundamentally improve RF performance. Secure Fast Roaming, VideoStream, and Wireless QoS improve application experience. No other industry solution offers the depth and breadth of the Cisco WLAN product family.

Unified Approach for Wired, Wireless, Remote, and Mobile Access

The Cisco BYOD solution strategy is to provide a common approach anywhere devices connect to the network, including wired, WiFi, public WiFi, and 3G/4G mobile and also regardless of whether the connectivity occurs in the main campus, branch office, home office, or mobile Teleworker location.

Unified Experience for End Users

The unified approach across network access types and locations, as well as the use of the Cisco AnyConnect client, provides a unified experience for users, which is consistent whether they are connecting at the corporate office over WiFi or remotely over 3G/4G mobile providers.

Unified Visibility and Device Management

Cisco ISE and Cisco Prime provide a single source and visibility for users and devices, simplifying troubleshooting and auditing.

Unified Communcations

Cisco UC and Cisco Jabber extend collaboration to BYOD devices, integrating users with corporate communications systems like voice, video, and conferencing, further extending their productivity.

Validated Solution Architecture

Finally, Cisco invests in validating that the BYOD solution architecture components integrate together seamlessly and provides validated design guidance and best practices to minimize deployment challenges. In addition, the BYOD solution is validated with other Cisco solution architectures.

Getting Started With BYOD

Deploy a Comprehensive Cisco BYOD Solution

As discussed, the Cisco BYOD solution is a comprehensive solution that addresses the key requirements and challenges for both the IT organization and for users. Key considerations for deployment are discussed to get started on planning and deployment.

Cisco provides validated designs and best practices to minimize deployment challenges. For more information, consult the Cisco Design Zone at: http://www.cisco.com/go/designzone.

Assessment and Deployment Services

Large or complex BYOD deployments can be challenging. To help, Cisco provides a comprehensive set of assessment, design, and deployment services to ensure your deployments are well planned and seamlessly rolled out.

For More Information

- Cisco Design Zone: http://www.cisco.com/go/designzone
- Cisco Adaptive Security Appliances (ASA): http://www.cisco.com/go/asa
- Cisco AnyConnect: http://www.cisco.com/en/US/netsol/ns1049/index.html
- Cisco Cius: http://www.cisco.com/go/cius
- Cisco Identity Services Engine (ISE): http://www.cisco.com/go/ise
- Cisco Jabber: http://www.cisco.com/go/jabber
- Cisco ScanSafe: http://www.cisco.com/go/scansafe
- Cisco TrustSec: http://www.cisco.com/go/trustsec
- Cisco Unified Access: http://www.cisco.com/en/US/solutions/ns340/ns414/ns742/ns815/landing_unified_access.html
- Cisco Wireless products: http://www.cisco.com/go/wireless