Cisco Enterprise Mobility Solution

Device Freedom Without Compromising the IT Network

Last Updated: March 7, 2014

Cisco Enterprise Mobility Solution

Cisco Bring Your Own Device

Introduction

Enterprises across the globe are continually working towards increasing their employee productivity, efficiency and flexibility. Mobility has moved up the priority list of several IT executives, who are expanding the pervasiveness of mobility initiatives throughout the organization. However, IT executives are challenged to support the significant increase in the number of mobile devices used by the workforce. On one hand, employees are demanding access from devices not only within the corporation, but also beyond the firewall with smartphones, tablets, home PCs, and laptops. On the other hand, risk management dictates that corporate data must remain protected. IT must adapt the ways in which they enable, manage, and secure end user access to enterprise resources based on the devices they are using, their role, resources they are allowed to access, places from where these resources are being accessed, etc. Getting mobile devices onto the enterprise network is now table stakes. Having a way to securely connect and monitor corporate owned and personal devices is one of the very first requirements for a network administrator. But, once you get mobile devices onto the network, finding balance is imperative, because it is more than just a matter of security. The evolution of integrating mobile device technology into business operations offers a platform for ongoing, cost-effective innovation that powers a more collaborative and productive workforce. Mobile wireless traffic is soon about to exceed wired traffic on a global basis and is comprised of mobile applications. As such, the volume, composition, and device-shift of mobile application traffic can pose a challenge to network administrators tasked with ensuring their quality and retain top talent—so what do you do? What features/functionality should you look for in order to ensure that once you allow users to connect their devices, that you can still ensure security, privacy, and productivity? The real challenge for IT is not only getting devices onto the network - it's what to do with them once they're there. Reporting on security compliance, ensuring the devices can use available services and assets and are restricted from those which they should not access, and making sure the devices do not overwhelm available network infrastructure. Enterprises are now beginning to see BYOD trend as an opportunity to enable comprehensive enterprise mobility. There is no longer any doubt that enterprise IT departments are adapting to mobile devices in the corporate workplace to meet user expectations and leverage new technologies to boost worker productivity.

The role of IT needs to balance security with productivity and coordinate business justification with the various lines of business (LOB) owners to implement mobility initiatives within an enterprise, with tools that help configure employees' mobile operating systems, syncs devices with a central server and manages the installation of applications, giving the IT organization the ability to support several types of devices yet still secure them. Almost 50% of Cisco customers lack support and guidance in this regards and are willing to invest in its deployment, using their early experience to quickly determine

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

what works and what does not and become more knowledgeable about how to target their the deployments. In Cisco's internal CYOD (Choose Your Own Device) implementation, the BYOD model is delivering tangible value to the corporation. Cisco IT spends 25% less on mobility per user with BYOD while supporting 28% more users and 82% more devices with 33% higher user satisfaction.

Mobility Market Landscape

Tablets and smartphones are turning into general computing devices with faster components and better integration and support in connecting to enterprise systems. They are being used by employees to perform their regular job functions. In many cases, each employee owns multiple devices (purchased themselves or employer paid) which they use for personal as well as business work.

The BYOD market was initially centered on allowing employees, partners, and guests to connect to the corporate networks and be able to perform a limited number of basic functions such as Internet access, access to corporate e-mail, calendar, and contacts, etc. As more and more personal devices become prevalent in the enterprise, workers are using these devices to access enterprise resources and applications to do their daily jobs. With employees using personal devices for mission critical job functions, mobile device management (MDM) and functions associated with MDM are becoming increasingly important. Functions such as ensuring that a device can be locked and remotely wiped in case it gets lost or stolen or when the employee is terminated are becoming a necessity. Recently, the market has in a sense gone beyond MDM, as mobile application management (MAM) and mobile information/content management (MI/CM) have become critical to user collaboration and productivity. As the number of devices, applications, and bandwidth demands grow, IT is challenged to manage the growth of mobile devices and traffic.

An enterprise's BYOD strategy should build momentum towards meaningful infrastructure, security, and wireless innovation and provide a solid rationale for BYOD investments. Developing a repeatable process for BYOD planning, delivery, measurement, course correction, and innovation positions an enterprise to handle the pace of change, to recognize transformational opportunities, and to respond with confidence.

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

Device Landscape

According to a recent Gartner Press Release, "With increased smartphone and tablet sales to consumers, a plethora of these mobile consumer devices, are invading the enterprise in a short period of time. According to a Gartner report this month (April, 2013) there will be a steady growth of smartphones. Overall, the total smart devices market is projected to grow 9% this year, to reach 2.4 billion units. Gartner expects a 7.6% decline in PC sales and said "This is not a temporary trend induced by a more austere economic environment; it is a reflection of a long-term change in user behavior." Mobile devices will likely slowly replace laptops."[1]

1. Gartner Press Release, Gartner Says Worldwide PC, Tablet and Mobile Phone Combined Shipments to Reach 2.4 Billion Units in 2013, April 4, 2013. http://www.gartner.com/newsroom/id/2408515.

Figure 1 Gartner Data on Device Shipments

Worldwide Devices Shipments by Segment (Thousands of Units)				
Device Type	2012	2013	2014	2017
PC (Desk-Based and Notebook)	341,263	315,229	302,315	271,612
Ultramobile	9,822	23,592	38,687	96,350
Tablet	116,113	197,202	265,731	467,951
Mobile Phone	1,746,176	1,875,774	1,949,722	2,128,871
Total	**2,213,373**	**2,411,796**	**2,556,455**	**2,964,783**
Source: Gartner (April 2013)				

293603

There are an increasing number of devices connected to the network, with each employee likely connecting many devices simultaneously. Many of those device will soon connect with Gigabit interfaces as 802.1ac wireless is enabled on newer mobile devices. With WiFi and 4G/LTE speeds increasing to Gigabits/Sec, one can easily foresee many new applications and use cases for BYOD.

Enterprise Network and Mobility

Enterprise mobility and the "consumerization of IT"—employees' use of consumer devices and cloud applications in the enterprise—are well under way across the globe. But IT organizations, particularly those in large enterprises, are struggling to keep pace with and respond to the impact of these trends-namely, the deterioration of the traditional security perimeter, the proliferation of endpoints that must be secured, and the intensifying demand by workers for anytime, anywhere access to corporate assets using mobile devices that they choose. IT administrators remain challenged in finding the optimal balance between securing sensitive corporate data and allowing employees to have access to the tools and information they need for productivity. Mobile devices are prone to loss and theft, which means so are the data and access credentials they hold. Employees using public networks to transfer data to mobile devices can put sensitive corporate information at risk. And users who access the Internet from their mobile devices are at constant risk of exposure to web-based threats, including data stealing malware. Finding balance is imperative, however, because it is more than just a matter of security. The evolution of integrating mobile device technology into business operations offers a platform for ongoing, cost-effective innovation that powers a more collaborative and productive workforce. In an increasingly connected world, embracing mobile technology will enable organizations to maintain their ability to not only compete, but also attract and retain top talent. The network is at the heart of all business functions and is a key enabler for service delivery. One of the key challenges for enterprises will be meeting the rapidly growing demands on their networks in a sustainable fashion. With the proliferation of mobile devices, BYOD, and network-attached devices, enterprise networks are getting more complex. Inconsistent management tools and policies across the wired and wireless segments of the network can increase the burden for network managers and drive up management costs and complexity. An architectural approach and design can help businesses realize greater levels of manageability, enhanced user/customer experience, greater levels of flexibility and performance, and improvements in security and policy.

Today enterprises have diverse wired and wireless LAN infrastructure implementations. The traditional workforce model involves a worker going to an office and performing their job functions while tethered to an IT-provided computer and an IP phone. Hence the focus has been on ensuring that the wired enterprise infrastructure is robust and secure. The wired network is built for high availability (HA) and performance, with adequate capacity and intelligent features such as QoS, to make phone calls, exchange data and video, etc., within and outside of the enterprise. Communication within the premises is based on a trust model, protected by firewalls at the perimeter and other security tools.

In contrast, the enterprise wireless infrastructure was built for convenience as an overlay, at least until the BYOD phenomenon emerged. With BYOD users will have three or more mobile/WLAN devices (laptop, tablet, phone) connecting to this infrastructure. The devices themselves could be user owned or corporate owned. What is the trust level of these devices that are accessing secure enterprise resources? How are they accounted for at all times? How do you apply policy and comply with security? How do you manage guest access, isolate and segment the network, and account for these diverse devices? One can expect a lot more focus on the wireless network. The WLAN needs to become as robust, secure, scalable, and predictable as the wired network to support BYOD.

Top of mind for most CIOs is security, mobility, productivity, cost savings, collaboration, and ease of operations. Based on our interactions with customers and available market literature, we believe roughly half of our customers fully understand what is required to implement and support BYOD. The other half have a moderate sense of the impact of BYOD implementation within their enterprise and would benefit from support and guidance in developing and implementing a BYOD strategy.

Mobile Device Security and Policy—Many enterprise CIOs and architects cite security as a major inhibitor in the deployment, adoption, and acceleration of mobile devices within their enterprise. It can be overwhelming to manage security for various applications for a huge set of new mobile devices with diverse OSes and users. Based on each customer's environment and business policy, there are many options for implementing and configuring personal and seamless remote access, network firewalls, intrusion prevention, anti-spyware, data security, device control for smartphones, desktops, and tablets for various user roles such as employees, guests, partners, and remote workers.

For these reasons, enterprises in the public sector (and some verticals in the private sector) have been reluctant to adopt BYOD. Public sector enterprises such as government and defense agencies have concerns about protecting confidential data that, if leaked, could create security problems. Some private sector enterprises, such as health care and finance, also need to comply with strict regulations. Many businesses however feel the pressure to stay competitive by embracing technology trends and offering employee-friendly environments. One way to accomplish the latter is to allow BYOD, which is a consumer-driven trend.

Policy management is critical to a successful mobility strategy which enables endpoint security for multiple devices and diverse user roles. Most enterprises now use an MDM to MDM-based remote wipe/lock that lowers risk. Application management and security are on the rise in a BYOD environment as enterprises seek to manage and secure applications rather than devices, with more granular policies applied based on worker or application type. More companies want enterprise application stores that allow for a central deployment method. In general, the BYOD security market extremely fragmented, with no one company dominating all the security aspects and needs of the enterprise. The security needs of a mobile workforce can be broken into:

- Ensuring that the devices used to access the corporate network are safe and are not jail-broken or rooted. They should not have threatening malware, spam, or applications that can compromise the corporate network or data.
- Making sure users and devices that are accessing the corporate network on-premise or off-premise can be identified and allowed connectivity only if they are authorized and meet company policy.
- How secure access with client-based or clientless access is ensured for data loss prevention with encryption or containerization with VPN optimized for efficient application delivery and capabilities.
- Device-level security functionality such as remote wipe/lock with integrated Network Access Control (NAC) ensuring that an action can be taken on non-compliant devices at any time (not just during access).
- Having visibility into users, devices, and the applications they are running on the corporate network.

Mobility—The hottest segment of the enterprise networking market is wireless LAN equipment to support enterprise requirements for user mobility and wireless devices. This trend has been pushing WLAN equipment sales and the trend is expected to continue to grow in the near future. As smartphones and tablets become more powerful, they are increasingly used by employees to connect to the WLAN and other enterprise resources to do their normal job functions. Mobile devices are reaching Gigabit speed with 802.11ac implementation in smartphones and tablets. The trend of WLAN upgrades for additional wireless capacity and performance within the enterprise network is required in the foreseeable future. Wired infrastructure is perhaps already over-built, WLAN upgrades make expansion much easier, simpler, and cheaper to upgrade the capacity of the enterprise infrastructure. It then becomes important for the WLAN to have same or similar intelligence and feature functionality, such as high availability, QoS, local switching, application visibility and control, ease of collaboration, etc., that users have become accustomed to on a wired infrastructure. Retail and utility verticals with mobile sales forces are adopting this trend faster than some other public sector and vertical segments. However, this BYOD mobility trend towards wireless deployment is considered to be more prone to security threats and must be seriously considered in your BYOD strategy. Investing in WLAN capacity, performance, and intelligent value-add features is a necessity, as discussed in the previous segment.

Collaboration—Many enterprises are expanding their mobility initiatives to include deploying and supporting a variety of mobile devices, mobile applications, and collaboration services. The fragmented corporate mobility environment is further complicated by BYOD programs which enable employees to use their personal smartphones and tablets at work. Successfully addressing the wide range of mobility initiatives requires firms to expand mobile application deployment to enhance employee productivity. Many firms are broadening the array of mobile applications deployed to enhance employee productivity. Mobile application implementation plans often vary for different types of devices. For example, enterprises are more likely to deploy presentation tools and spreadsheet applications over tablets. In addition, there is emerging demand for video, streaming, and web-conferencing applications to facilitate employee collaboration and communication capabilities over these mobile devices.

Network Intelligence—Fueled by BYOD, remote working, productivity initiatives, and cost cutting have all made network intelligence a very important topic in recent times. Application intelligence and the signatures used for it are difficult areas for IT to manage. Many customers see value in having identity, device, and location information included in reports for application intelligence via integrated network management functions. Consider these capabilities and answer the following questions for BYOD implementations:

- Application Visibility—What applications are running over my network globally and in a specific site? What is the actual application (and not just a basic determination based on port number)?
- Application Performance—What is the throughput breakdown for each of the applications on the network over a period of time within a specific site and across sites? What are the response time components of a flow associated with a client-server pair for a specific application? What is the measured latency and loss for a specific flow, for a specific application, for a specific site, or over a specific WAN link?
- Application Optimization— How much compression was applied by WAN Optimization? How much latency reduction was provided by the use of WAAS? How do these impact the overall application performance metrics measured (application performance)? What is the resultant performance improvement (X-factor or percentage)?
- Application Control—How do I allocate bandwidth to jitter/delay sensitive applications as well as those that are bandwidth sensitive? How do I provision a control policy globally while taking into account per-site metrics such as available bandwidth? How do I create an over-arching global SLA for application performance and ensure that application control normalizes applications to this SLA for performance consistency? How do I block applications that should not be allowed on my network?

Role of MDM/MAM in the Enterprise Network

Many enterprises are using MDM, which is designed to help an enterprise rapidly and securely deploy mobile devices, tablets, and applications with policy, compliance, configuration, and application management to ensure lower TCO and minimize risk. MDM is about enabling, facilitating, monitoring, and securing users, devices, content, and applications, while considering relevant parameters such as various device types with diverse OSes and user roles and locations in a BYOD implementation. Large enterprises are extremely interested in delivering general-purpose as well as custom-built corporate applications to their workforce (for example, mobile sales force automation applications). While MDM providers may not be directly involved in application development, they can provide appropriate solutions to help customers distribute and manage corporate-specific (and corporate-approved) mobile applications for smartphones and tablets, and eventually for other connected devices, in healthcare, manufacturing, oil and gas, and other industries.

BYOD security and device management are the foundations of an enterprise BYOD strategy which must consider all mobile worker types and functions before deploying solutions. Organizations need to consider solutions across the security sub-segments that secure endpoints, provide protection for the corporate network, and protect data as it moves over their infrastructure. End users need to be aware of and understand corporate BYOD policy for a a successful, secure enterprise mobility roll out. MAM is also picking up relevance in enterprise mobility as enterprises shift their focus from mobile device management (now somewhat commoditized) to mobile application development, delivery, and security. Start-ups are gaining ground and developing key partnerships with established players and forming an eco-system to deliver holistic solutions. Established players are moving quickly to capture market opportunity. Many high profile MDM/MAM companies are seeing extensive venture funding and some have been acquired by more established companies within the last one year.

The adoption of corporate application stores is also increasing rapidly. Large enterprises are extremely interested in delivering general-purpose as well as custom-built corporate applications to their employees.

The ability to integrate MDM functionality, coupled with a policy-based network access, ensures that legitimate devices and users can access the network and attempted violations can be controlled by prohibiting or limiting access to the network or network resources.

In conclusion, with multi-technology project initiatives such as BYOD that touch upon infrastructure, mobility, manageability, security, and policy control, the decision to invest in full BYOD deployment is increasingly shifting from IT alone to the various LOB owners. IT now needs to drive the overall coordination and alignment of business strategy with clear ownership and cross-discipline participation.

User Need and Role of IT

BYOD connectivity may look like a simple extension of enterprise mobile services, however broad user expectations and the diversity of devices create unique infrastructure demands and challenges for IT operations with end-to-end and network optimization and lifecycle management to support mobility. With the growing adoption of personal devices, COPE (corporate-owned personally-enabled), and company managed mobile devices by employees in the workplace and an increased acceptance from executives and IT managers, the workspace of the future needs to cater to the demand for increased consumerization, mobilization, and virtualization and requires additional features, capabilities, and tools to further facilitate worker productivity and ease of use, while adhering to company policies and security guidelines.

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.

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 mobile collaboration devices. 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.

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.

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.

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.

In summary, key IT functions can be summarized as:

- Provisioning and configuration—Ability to rapidly onboard the employee devices with the right setting, configure the right network settings and parameters, and push mandatory applications that ensure employee productivity.
- Security and compliance—Device security policies, password protection, timeout and auto-locking, data loss prevention, data at rest, and data in transit
- Operations and support—Helpdesk and troubleshooting, self-serve user consoles, proactive compliance and policy implementation
- Reporting and feedback—Real-time usage reports and dashboard, detailed insight into device and user inventory integration with Security Information and Event Management (SIEM) solutions
- De-commissioning of devices—Inventory auditing and identification of inactive devices (and users) and full or selective device wipe

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 and applications to do their work. 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.

Cisco's Enterprise Mobility Architecture and Customer Capabilities

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

The Cisco Enterprise Mobility Solution delivers increased business efficiency/productivity and agility by providing users with consistent, seamless, and secure access to any combination of applications, content, and communication on any device in any location across any wired or wireless/mobile network. The comprehensive solution backed by validated designs, services, and a solution roadmap combines Cisco's network, security, collaboration, data center, and management technologies with partner technologies to deliver an end-to-end solution that meets users' evolving mobility and device needs. The Cisco EM Solution has a broad portfolio of products that bring together and integrate the best in class technologies, expertise, and partner ecosystem required to offer a complete mobility solution and services portfolio that empowers people to adopt the most collaborative, productive, and unbound work styles. The EM Solution CVD program consists of systems and solutions designed, tested, and documented to facilitate faster, more reliable, and more predictable customer deployments.

Additionally, with Cisco professional and technical support services and a broad portfolio of network infrastructure elements and partner components, customers can build and support their network with:

- Policy-enforced, highly secure access
- Exceptional wired and wireless network experiences
- Productive and seamless collaboration with WebEx, Jabber, and other applications
- Simplified operations and better experience with a lowered total cost of ownership (TCO)

When Mobility within an Enterprise is properly implemented, it delivers an uncompromising, work-your-way user experience and enables organizations to secure data with unified policies and essential controls. To solidify IT as a key contributor in driving better business processes, IT teams must shift from maintaining the network to delivering innovative, connected experiences. The key to success is to simplify the network to:

- Scale the business to meet new mobility demands with faster service rollouts and efficient change management.
- Simplify and converge the access network to provide more network services, greater consistency, and an open, programmable infrastructure.
- Deliver a single policy across wired, wireless, and VPN, managed and BYOD assets, and multi-mobile device management (MDM), Mobile Application Management (MAM), and Mobile Information Management (MIM).
- Achieve access lifecycle management and granular visibility that streamlines infrastructure management tasks and improves the end-user experience.

This white paper summarizes the current BYOD landscape and market trends, user requirements, and IT challenges and describes new customer capabilities that have been added to the Cisco BYOD Smart Solution to strengthen and accelerate customers' BYOD deployments.

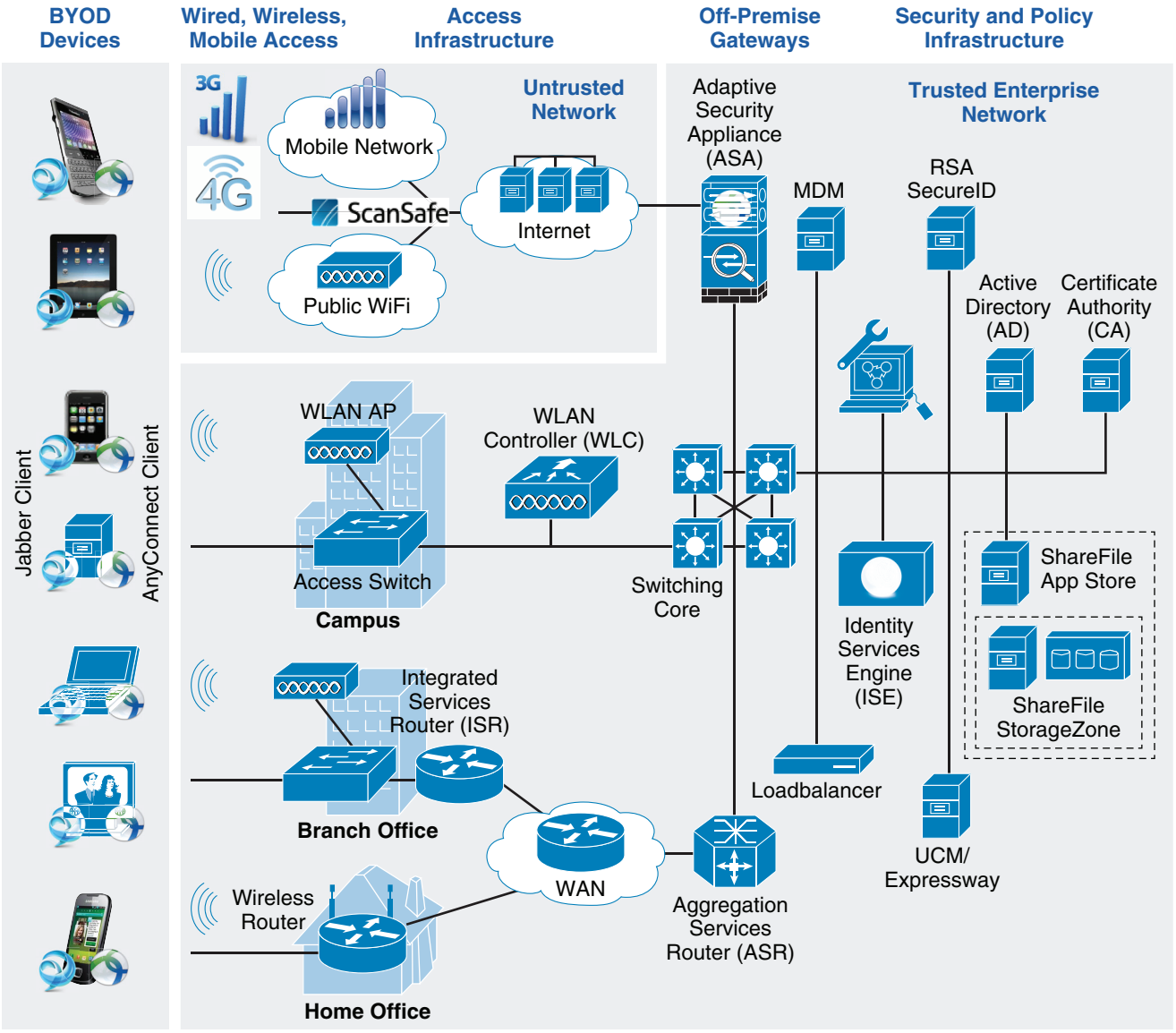
High-Level Solution Architecture

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

Figure 2 HIgh-Level BYOD Solution Architecture



Cisco Solution—New Components

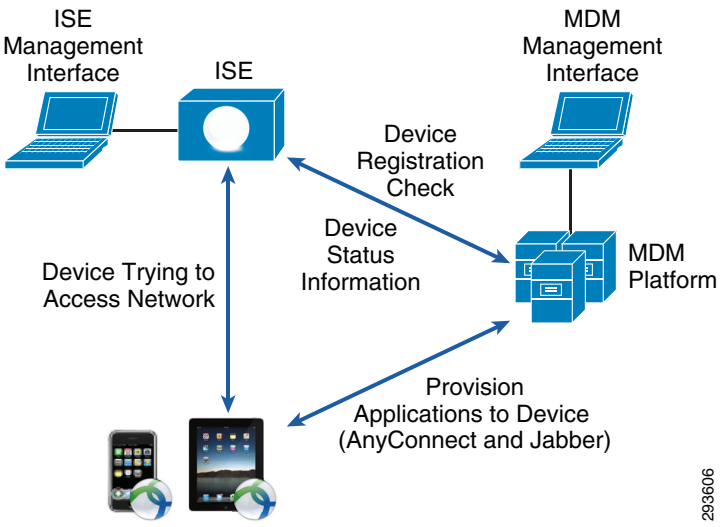
The sections which follow outline the various new Cisco components of the solution architecture and the role they perform.

The Cisco BYOD solution continues to add new functionality and customer capabilities to address deployment needs. Some of the capabilities include:

Integration with third-party Mobile Device Management (MDM)—Integration between Cisco Identity Services Engine (ISE 1.2) and MDM partner platforms enables posture, compliance assessment, and network access control of mobile endpoints attempting to access the network. The solution also

performs on-going posture checks to ensure compliance and that the correct network access level is maintained. The Cisco solution is composed of ISE with an Advanced Feature License and an MDM platform from one of our supported MDM partners—as of Cisco ISE Release 1.2, AirWatch, Good Technology, MobileIron, SAP Afaria, XenMobile, and Fiberlink.

Figure 3 Seemless Connectivity and Integrated Security



Integration between ISE and its MDM partners is accomplished by:

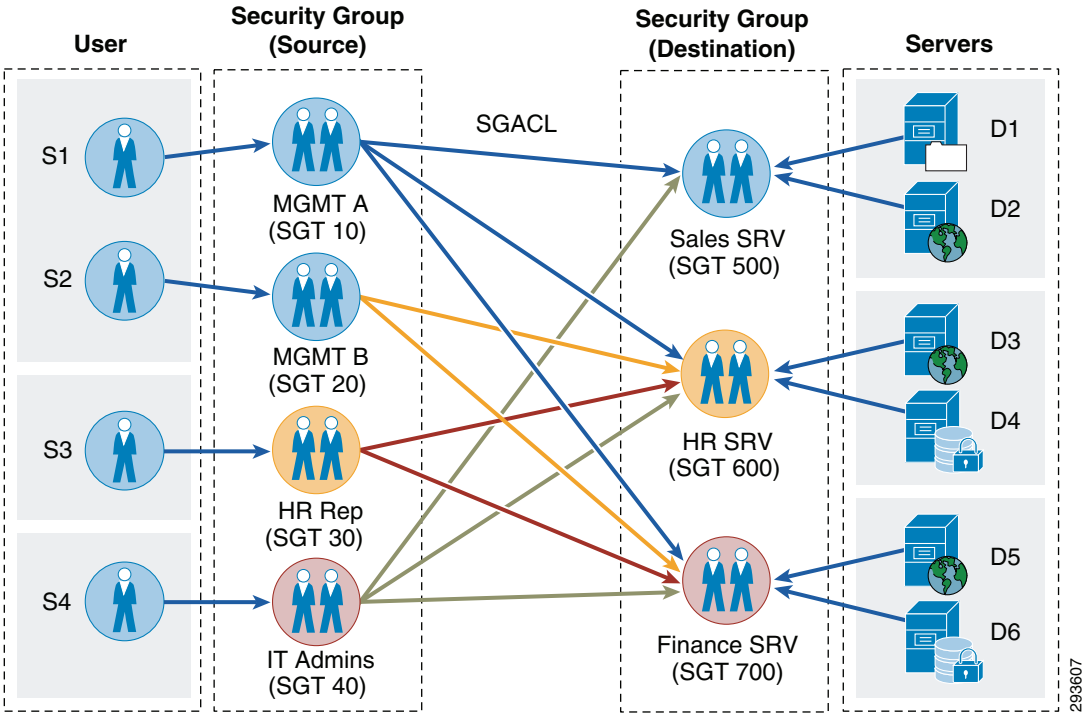
- Cisco ISE profiling devices as they attempt to access the network. Through this process various types of mobile devices attempting access are discovered.
- Mobile devices are subjected by Cisco ISE to security posture assessment as specified by IT policy. Cisco ISE queries for posture information associated with mobile devices as collected by the MDM partner platforms.
- Cisco ISE enforces access policy based on the posture status reported by the MDM partner platforms. The access policy may be constructed on specific attributes within Cisco ISE or at a global level of "in compliance" or "not in compliance" within the respective MDM partner platform.
- End-users can manage the status of their devices via the Cisco ISE "My Device" portal. Through this portal end users can lock, suspend, or un-enroll devices in the event they are lost or replaced. Cisco ISE can perform these functions natively or by integration with the MDM partner platforms. Specific posture attributes collected by MDM partner platforms for compliance and access policy enforcement in Cisco ISE are:
  - Is the mobile device registered with MDM?
  - Does the mobile device have disk encryption enabled?
  - Does the device have PIN lock enabled?
  - Has the device been jail broken/rooted?
- Global compliance-posture compliance decisions may also be made by the MDM platform instead of Cisco ISE. In this scenario additional attributes, such as blacklisted applications or presence of an enterprise data container, may be checked. The MDM platform simply informs Cisco ISE if a device is in compliance or not and then Cisco ISE enforces the appropriate network access policy.

TrustSec Secure Group Access (SGA)

Cisco TrustSec® helps organizations secure access to their networks and networked resources with policy-based access control, identity-aware networking, and data integrity and confidentiality services. Cisco TrustSec enables organizations to improve compliance, strengthen security, and increase operational efficiency. Administered by ISE, TrustSec provides for an appliance-based overlay solution later in the roadmap and as an integrated 802.1X infrastructure-based service designed to extend access enforcement throughout the network.

Previously, traditional techniques such as dACL and VLAN override alone were used to enforce policy of BYOD access. Smart Solution 2.0 TrustSec SGA provides a more scalable and easier to configure method. Cisco TrustSec simplifies the provisioning and management of secure access to network services and applications. Compared to access control mechanisms that are based on network topology, Cisco TrustSec defines policies using logical policy groupings, so secure access is consistently maintained even as resources are moved in mobile and virtualized networks. De-coupling access entitlements from IP addresses and VLANs simplifies security policy maintenance tasks, lowers operational costs, and allows common access policies to be consistently applied to wired, wireless, and VPN access.

Figure 4 TrustSec Secure Group Access Simplified Policy Enforcement



Converged Access

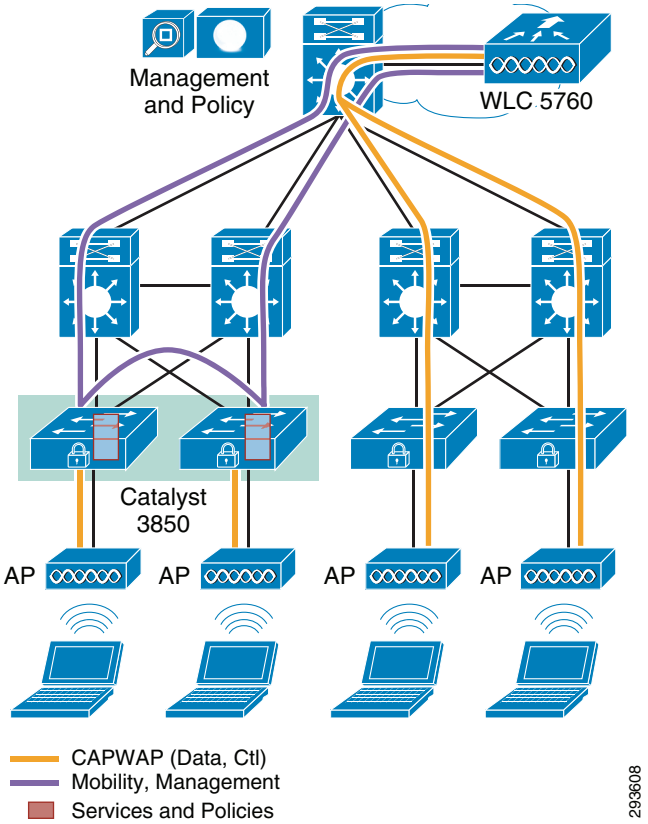
IT organizations are struggling to manage the BYOD trend and the growth of mobile devices and traffic. They face two main challenges:

- The complexity of managing separate wired and wireless networks, multiple management systems, multiple network operating systems, and chaotic device onboarding processes.

- The inconsistency of wired and wireless architecture, policy, security, features, and operations. When compared with wired networks, wireless also does not have the same level of granular QoS, policy, and security enforcement close to endpoint devices.

Converged wired and wireless network with one logical infrastructure increases business agility, simplicity, and scale and delivers greater operational efficiencies. The Cisco Catalyst 3850 switch is the converged access switch with integrated wireless controller functionality and is the foundation of the unified wired and wireless network. Wireless access points can be terminated directly on the Cisco Catalyst 3850 switch, which means termination of the Control and Provisioning of Wireless Access Points (CAPWAP) data and management tunnels to natively convert wireless data traffic (802.11) to wired traffic (802.3) or vice versa. This convergence is further enhanced by the new switch's capability to support robust wireless throughput bandwidth, up to 40 Gbps on the Cisco Catalyst 3850 switch and 60 Gbps for the 5760 wireless controller, thereby making the network capable of addressing the proliferation of mobile data. Such wired-wireless convergence at the network edge also brings a high level of visibility and policy consistency to the entire network, which did not exist in the past. The benefits of converged access also include high-throughput performance where the wireless data plane is terminated at the network edge, which meets the triple demands of high wireless density, bandwidth-hungry video applications, and highly-capable smartphones. The Cisco Catalyst 3850 switch and the 5760 wireless controller perform at line rate in spite of the number of clients because wireless data tunnels are terminated in hardware. In addition, Cisco is able to bring more than 20 years of Cisco IOS Software technology excellence to the wireless network that was previously only available on the wired network.

Figure 5 NGWC—Converged Wired/Wireless



Converged Access Management

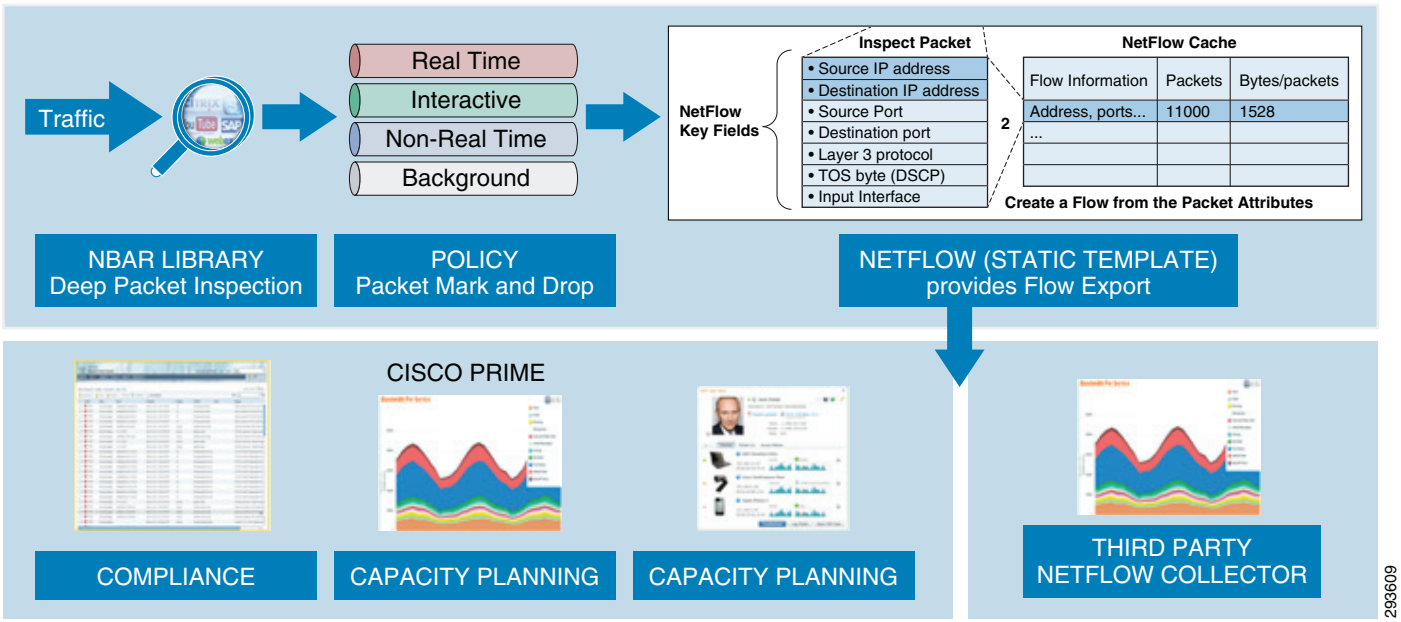
Cisco One Management provides comprehensive lifecycle management, performance assurance, and compliance for converged wired and wireless networks. Cisco One Management simplifies network management operations. Cisco Prime™ infrastructure provides a central platform for integrated lifecycle management and visibility of applications and services across wireless, wired, campus, and branch network infrastructure.

Mobile Application Visibility and Control (AVC)

With many new mobile devices joining the enterprise WLAN network, visibility into mobile applications is becoming critical. CUWN WLC from R 7.4 and above adds AVC capability based on NBAR2 application recognition, which gives customers better ability to manage mobile traffic, including prioritizing business applications, limiting personal applications, and blocking unwanted applications. Cisco AVC has the following uses:

- Classifying and marking wireless mobile device applications, identifying and differentiating real-time voice, video, or business-critical applications from lesser important—but potentially bandwidth-hungry—applications so as to prioritize, de-prioritize, or drop specific application traffic.
- Capacity planning and trending—Baselining the network to gain a clearer understanding of what applications are consuming bandwidth and trending application usage to help network administrators plan for infrastructure upgrades.

Figure 6 BYOD and Mobile Applications



Bonjour Application Gateway

This section provides a brief overview of the Cisco Wireless LAN Controller software Bonjour Gateway feature to manage Apple's Bonjour protocol in a BYOD enterprise context.

Bonjour is Apple's zero-configuration protocol for advertising, discovering, and connecting to network services like file sharing, print sharing, media sharing, etc. The Bonjour protocol was originally designed for home network use and utilizes Multicast Domain Name Services (mDNS) via link-local multicasting to share network services. While this approach works well in home networks, a limitation of link-local multicasting is that these network services will only be shared within a single Layer 2 domain (such as a VLAN or WLAN). In a BYOD enterprise scenario, different WLANs and VLANs are used for different classes of devices, including corporate devices, employee devices, personal devices, and guest devices (as well as quarantine WLANs for unapproved devices). As such, basic Bonjour operations—such as printing to a wired printer from a wireless LAN—may not be natively supported.

To address this limitation and to facilitate the user demand of BYOD for Apple devices within the enterprise, Cisco has developed the Bonjour Gateway feature for its Wireless LAN Controllers (WLCs) and Catalyst switches. This feature solves the Layer 2 domain limitation for Bonjour by allowing the WLC or Catalyst switches to snoop, cache, and proxy-respond to Bonjour service requests that may reside on different Layer 2 domains. Additionally, these responses may be selectively controlled by administrative policies, so that only certain Bonjour services will be permitted in specific Layer 2 domains.

Application Virtualization Clients

Many customers want to leverage application virtualization clients to provide access to legacy applications (e.g., Microsoft Office) or for data security. This release validates Citrix Receiver on mobile tablet devices that are on-boarded with the Cisco BYOD Smart Solution. Citrix has upped its investment and priority on Mobility with several new acquisitions and enhancing the receiver Client to Worx. Cisco and Citrix are partnering to validate a new Mobility Workspace integration and validation based on a more user friendly and comprehensive architecture.

Jabber Integration

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. We continue to improve the user experience of Cisco Jabber on mobile devices participating in the BYOD system with each release and offer guidance to customers on achieving the best user experience.

This is broadened handset coverage in the solution validation, including the latest devices/OS versions from Apple and Samsung.

Key Advantages of the Cisco Enterprise Solution

- Fully integrated, centralized, single point of visibility and control—All Cisco networks (fixed or wireless, real or virtual, on or offsite) integrated to one control panel, resulting in greater security and ease of management.

- Fully integrated, centralized, single point of visibility and control—Fully integrated, centralized, single point of visibility and control of users, devices, location, network, and applications.
- High quality and secure collaboration through Jabber video and voice clients.
- Services across end-to-end partner ecosystem—Pre-integrated and tested solutions with world-class partners. End-to-end service support foundational blocks enabling customers to unlock value from their existing investments.
- Future proofing:
  - Full gamut of use cases
  - Device agnostic
  - Scalability
  - No static infrastructure siloes

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 such as flexibility to allow for multiple diverse user groups, such as deskbound or mobile workers, customers, guests, etc. It creates a device- and OS-agnostic platform for scaling.

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 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 Enterprise Mobility 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.

The dependence on Wi-Fi for everyday business has put more demands on enterprise networks. More and more, networks need to provide faster speeds and more Wi-Fi capacity than ever before. Challenges ranging from BYOD access to the growth of bandwidth-hungry applications such as video are having an impact on all industries. To address the growing demand for bandwidth and the need for speed, the IEEE has come up with the next generation of Wi-Fi: 802.11ac. The first wave of the 802.11ac standard will offer a three-fold performance increase over 802.11n. Through a variety of enhancements, 802.11ac offers:

- Wider channels—80-MHz channel width when compared to 802.11n MHz. Wider channels provide more bandwidth.
- An increase in spatial streams—The 802.11ac standard allows for up to eight spatial streams, compared to the four offered by 802.11n.
- Ability to operate in the less crowded 5-GHz band—Most Wi-Fi today uses the 2.4-GHz band, in which clients are susceptible to interference from other clients. The 2.4-GHz band also has fewer channels than the 5-GHz space.

Customers are demanding seemingly "instantaneous" data transfer experience and a pipe fat enough to deliver high quality of experience (QoE). 802.11ac will deliver higher levels of performance that are commensurate with Gigabit Ethernet networking in the Enterprise for:

- Delivering network with enterprise-class speeds and latencies.
- High-density environments with scores of clients per AP, which are exacerbated by the BYOD trend such that one employee might carry two or even three 802.11 devices and have them simultaneously consuming network resources.
- The increased adoption of video streaming.

802.11ac is about delivering an outstanding experience to each and every client served by an AP—even under demanding loads. No other industry solution offers the depth and breadth of the Cisco WLAN product family.

As more business critical applications are being deployed over WLANs and the wireless network is being used as the primary access medium (rather than an overlay network), high availability is becoming critical to key verticals such as healthcare, manufacturing, higher education, and retail (high availability equates to survivability in retail). Not just at the Access Point, but SSO at a Client level will ensure that the AP sessions are intact after switch over.

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 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 Communications

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.

Deploy a Comprehensive Cisco BYOD Solution

CIOs are focused on understanding the impact of BYOD solutions, but they are struggling to understand the cost-benefit of evolving their program from a basic deployment to one where they can reap the total benefit of the Cisco portfolio of products and technologies in a solution that has been fully tested in an end-to-end system. Cisco can be a trusted advisor to help technically and strategically implement BYOD solutions within an enterprise, whether you are starting a new BYOD deployment or evolving your BYOD program from a basic deployment to an enhanced or advanced deployment. Cisco can help companies define, implement, and manage a BYOD solution. Cisco Services can assist with BYOD policies to implement a broader mobile enablement for a company. The Cisco BYOD solution is a comprehensive solution that addresses the key requirements and challenges for both the IT organization and 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, see 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 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 Unified/Converged Access: http://www.cisco.com/en/US/partner/prod/collateral/switches/ps5718/ps12686/white_paper_c11-726107.htm
- 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
- Cisco 82.1ac Use Cases: http://www.cisco.com/en/US/prod/collateral/wireless/ps5678/ps13367/at_a_glance_c45-729588.pdf