

## Tablets Welcomed.

### How to Get Any Device, on Any Network Reliably and Securely.

Knowledge and service worker productivity is in the midst of a profound transition enabled by increased levels of true mobility. Highly portable, connected devices and applications harvesting network intelligence are quickly changing business and organizational models. They are also changing employee habits and the way we work.

Undoubtedly, one of the most important drivers of this change has been the introduction of very user-friendly tablet computing devices, such as the Apple iPad. It is increasingly observed that tablet users depend on these devices for a variety of daily tasks, and much like the smartphone, the tablet is becoming an indispensable tool that follows users throughout the day.

#### Tablet Computing Trends

For many users, these devices are “good enough” and may be regarded as even better productivity tools than traditional computing platforms, such as laptops. As a result, tablets are quickly making their way into the enterprise. Three main trends seem to emerge in the way enterprises handle the influx of these devices.

##### Sponsor

The most enlightened companies provide tablets to their employees as their primary computing device and even go as far as developing custom applications that solve critical business problems. In the process, these companies gain a competitive advantage. This category of companies is taking a still largely consumer device and converting it into a managed device that they have full control over. Deloitte Consulting estimates the percentage of tablets purchased by enterprises to equal 25 percent of all tablets sold, while Forrester puts that same number at 30 percent. Whatever the true number may be, it is certainly a trend that is here to stay.

##### Embrace

Several companies realize that employee productivity is highly dependent on employee satisfaction, which is in turn influenced by the employee’s ability to use a mobile device of their own choice. As a result, these companies allow their employees to “choose” what type of mobile device they prefer instead of forcing them into an already set menu of choices. This trend is widely referred to as “bring your device to work” or BYOD. There are two flavors of BYOD emerging:

- **Unmanaged devices:** This is the most popular version because it does not require any IT resources. It is also cheaper because the company does not have to buy or reimburse the user for the device.
- **Managed devices:** Some companies will choose to reimburse (up to a dollar limit) employees who buy their own device, and in doing so will require that specific security requirements are met with that device. The main difference between this category and the Sponsor category is that the employee ends up owning the device at the end of its useful life.

---

## Ignore

At the other end of the spectrum, a lot of companies still ignore the fact that employees bring their “consumer device” to work. These companies are putting their networks at risk by not instituting controls on how these devices access network resources. If they prohibit the use of those devices on the corporate network, they are putting employee good will at risk.

## The Challenges

The influx of tablets in the enterprise brings a variety of challenges that IT departments need to address. These challenges may vary depending on where the user is (on or off premises), what type of device they are using (managed or unmanaged), or what type of network access they have (wired or wireless).

We group the challenges in three categories.

### User Experience and Utility Challenges

Companies that either sponsor or embrace tablets are certainly looking to maximize their ROI from those devices and make employees as productive as possible. With the majority of these devices able to connect only through the wireless network (most of them lack an Ethernet port), the importance of a robust wireless infrastructure is paramount. So what impacts end-user experience and utility?

### Video

Tablets are largely adopted because of their amazing capabilities at producing interactive multimedia experiences. We are seeing:

- Hospitality companies empower their concierge employees with interactive multimedia to showcase things to do around town.
- Retailers enhancing the customer experience with mobile video expert help.
- Healthcare companies providing visualization tools to doctors at a level of clarity and portability never before available.

To provide streaming video (often high definition) on a tablet, a wireless network needs to effectively handle multicast video streams to multiple endpoints.

### Intelligent Applications

Companies that deploy tablets realize the potential of changing their business processes by taking advantage of the developer network, and in many cases building their own custom applications to solve complex operational problems. These applications become even more productive when they can take advantage of network-provided intelligence. For example, when a manufacturing company builds an application for the shop-floor foreman, contextual awareness providing real-time location information about critical production assets can be incorporated into that application, immediately improving the ROI.

---

### Bandwidth Availability

Wi-Fi, the primary network access method for tablet devices, is a shared resource. As more and more devices enter the network, this shared resource is stretched thinner and thinner.

- The average enterprise employee may now carry three or more networked devices (laptop, smartphone, tablet, handheld scanner, Wi-Fi phone, and so on). Improved portability creates a high-client-density issue that can significantly impact user experience.
- The problem becomes even more exacerbated when you consider that many devices are running virtual desktop applications in an effort to reduce security threats. Virtualized desktops have bandwidth bursts during session initiation and at frequent intervals, placing even greater demands on bandwidth availability.

### Roaming

In contrast to laptops, which one can't really operate while walking, tablets are more like smartphones, in that they allow users to be productive even while moving. As the number of clients roaming between access points grows, the wireless network is experiencing increasing pressure. This, in turn, makes producing a seamless mobility experience even more challenging, especially in cases where the network is not fully equipped to handle this level of mobility.

### Security Challenges

It almost goes without saying that to be useful to users, the network needs to provide a strong and secure connection. Obtaining a secure connection and provisioning the right access criteria can be one of the biggest challenges IT will have to solve with tablets, particularly when dealing with unmanaged devices. The main security challenges can be summarized as follows.

#### Profiling and Posture

Unmanaged devices are inherently risky and should be carefully screened for the right security updates and patch levels before being allowed onto the network. It is critical to avoid the spread of malware and to protect sensitive corporate data.

- Device profiling (or fingerprinting) is an essential tool used to determine what the device is so that it can be treated accordingly
- Device posture assessment is an essential step in minimizing the risk of viruses and malware spreading to other network resources when the device accesses the network. Noncompliant devices can be denied access, placed in a quarantined area, or given restricted access to computing resources. This is critical for keeping nonsecure devices from infecting the network.

#### Policy Assignment

Once a device is authenticated on the network, IT needs to determine the level of access that device is granted. Policy is typically dependent on variables such as who the user is (role in the organization), what device is used, where and when access is permitted, and any other attributes the company decides on. Policy is used to manage a large number of users with as few resources as possible. Typical policy options that companies may consider are:

- Employees can access everything from either corporate or personal devices, but nonemployees are blocked.

- 
- Employees are required to use corporate devices. Personal devices are not allowed, and there is no guest access.
  - Employees can access all resources from corporate devices. Employees using personal devices and nonemployee partners have restricted access.

#### Off-Premises Access

If you have allowed access to that employee owned device, an important question is what happens to the sensitive corporate information that is now on the device, while the device is being used off-premises? The risks are many:

- The device may be lost or stolen, allowing any perpetrator to gain access to corporate information.
- The employee may not be the only user of the device.
- The device may unknowingly be connecting to unsecured (and possibly malicious) networks at airports or coffee shops.

#### Threat Defense

The threat landscape is constantly changing, and while device postures can help to ensure that the latest security updates are installed, this does not prevent an infected device from entering the network. A multilayered security approach is needed to protect users against:

- Infected websites, which make up the majority of endpoint infections today
- Port 80 malicious traffic, such as social engineering threats through instant messaging or Web 2.0 applications

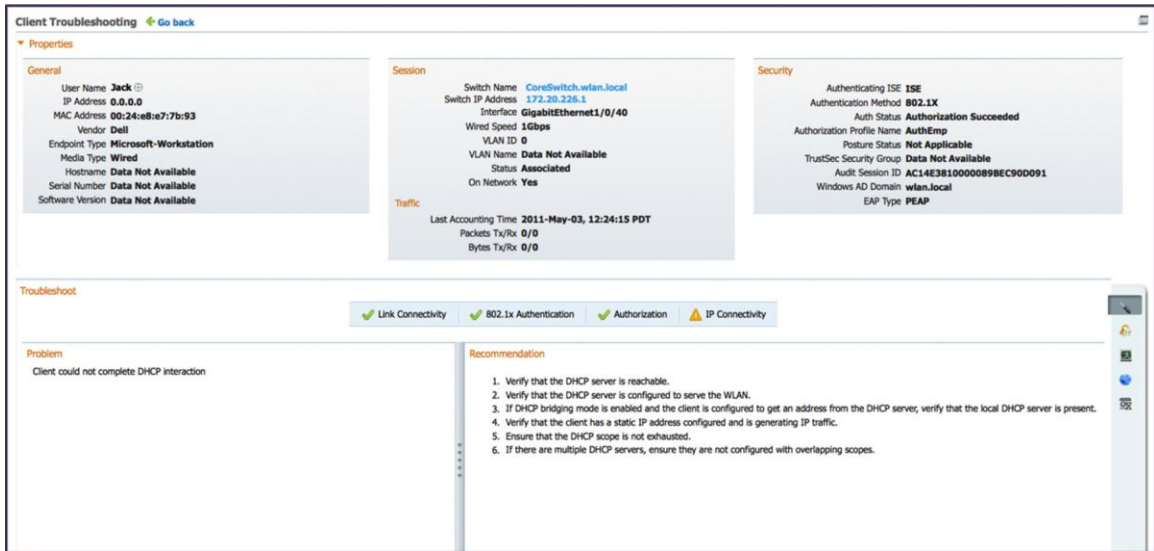
#### Manageability Challenges

Typical IT departments see their resources quickly drained from the increasing needs for device management and troubleshooting. In many cases (especially before the BYOD era), those demands could exceed 25 and even 30 percent of IT budgets.

#### Troubleshooting

Unmanaged devices present an even bigger problem, particularly when employees call the help desk to demand problem resolution. It is therefore critical that IT maintain high visibility into all devices accessing the network. IT must avoid the taxation of resources that is bound to come from this client wave. Figure 1 shows how the Cisco Prime Network Control System (NCS) consolidates wired and wireless client troubleshooting under a single management tool.

**Figure 1.** Wired and Wireless Client Troubleshooting on the Cisco Prime Network Control System



### Capacity Planning

The influx of tablets in the enterprise also poses a huge planning challenge for IT staff. Having a historical point of view into the types of devices in your network, their relative growth, and the demands they place on your network is a vital component of actionable capacity planning.

### Guest Access

Just as you may have unmanaged devices such as tablets accessing the network, you may also have unmanaged users (guests/visitors) requesting access. Effective network management should be integrated to include all device and user combinations.

### The Cisco Solution

Cisco® Borderless Networks is the architectural approach required to meet all the challenges we’ve just described. Table 1 summarizes the components making up the solution.

**Table 1.** How the Cisco Solution Meets the Challenges

| Challenges                  |                  | Solution Elements   |
|-----------------------------|------------------|---|
| User Experience and Utility | Video            | <p><b>Medianet with Cisco VideoStream:</b> Enables the efficient conversion of multicast video streams into unicast streams at the access point. Utilizes stream prioritization and resource reservation control to optimize video delivery and help ensure high-performance for the largest number of clients.</p> <p><b>Cisco Compatible Extensions:</b> This industry-leading program helps to ensure that the majority of Wi-Fi devices on the market today pass stringent interoperability testing that optimizes performance, including video.</p>  |
|                             | Intelligent Apps | <p><b>Context-aware software:</b> Provides network intelligence such as location-based services, and other types of monitoring (for example, temperature, shock, humidity, and so on) through third-party partners. Because this software uses an open API, information can be exported and used for a variety of applications from the Cisco Developer Network. These applications can significantly enhance the tablet user experience.</p>   |
|                             | Bandwidth        | <p><b>Cisco CleanAir technology:</b> Wi-Fi, an open standard, is subject to interference from a multitude of devices that impact network performance. Cisco CleanAir technology is a self-healing system that can detect, classify, and mitigate RF interference to optimize performance.</p> <p><b>Cisco ClientLink:</b> Most new mobile devices come with a dual 802.11n radios. However, legacy devices (still prevalent in corporate networks) may only operate in the 2.4-GHz band. For those devices, Cisco ClientLink can optimize performance (throughput) by up to 65 percent, and as a result improve overall airtime fairness and performance.</p> |

| Challenges           |                       | Solution Elements  |
|----------------------|-----------------------|--|
|                      |                       | <b>Cisco BandSelect:</b> Any client with dual radios will be pushed to the less crowded 5-GHz frequency, freeing up space in the 2.4-GHz frequency for older devices.  |
|                      | Roaming               | Cisco wireless network solutions support both Layer 2 and Layer 3 roaming for a variety of mobile applications including voice. Video conferencing through popular tablet applications such as Cisco WebEx <sup>®</sup> , Facetime, or Skype.  |
| <b>Security</b>      | Profiling and Posture | <b>Cisco Identity Services Engine (ISE):</b> Profiles the device requesting network access as managed or unmanaged. It subsequently assesses the device's posture, and if the device is healthy, ISE admits the device to the network with secure authentication.  |
|                      | Policy Assignment     | <b>Cisco Identity Services Engine:</b> Enforces wired or wireless client policy by assigning users and devices the right quality of service (QoS), on the appropriate VLAN, such that IT can easily monitor where, how, what, and when the user or device can access the network.  |
|                      | Off-Premises Access   | <b>Cisco AnyConnect™ Secure Mobility Solution:</b> Protects device connections all the time by automatically creating a secure tunnel (VPN) through any Wi-Fi connection when the device is off-premises. Particularly important when the device may be connecting to unsecured networks.<br><b>Cisco Prime Network Control System (NCS):</b> A lost or stolen device can be quickly removed from the approved device list so that the missing device can't gain network access (wired or wireless) again.   |
|                      | Threat Defense        | <b>Cisco AnyConnect Secure Mobility Solution:</b> Protects mobile users from web-based threats and enforces consistent web security policy using Cisco's premises-based Cisco IronPort™ Web Security Appliances or Cisco ScanSafe Cloud Web Security.<br><b>Cisco Security Intelligence Operations (SIO):</b> Provides real-time global threat visibility and automatic protection to Cisco security deployments.  |
| <b>Manageability</b> |                       | <b>Cisco Prime Network Control System (NCS):</b> Provides unified visibility into the converged wired and wireless access network. Significantly reduces deployment and management costs associated with device troubleshooting by consolidating the information under a unified view.<br><b>Cisco Identity Services Engine (ISE):</b> Integrates guest access functionality, empowering employees to sponsor visitor access in a simplified interface. Provides an isolated secure connection to the network, as well as complete auditing and accountability of the guest. |

The most prevalent use case that IT departments need to provide solutions for is when an employee brings their own personal device into the company and seeks to gain network access. As outlined earlier, Cisco has a comprehensive solution that allows an unmanaged device to get onto the network (regardless the access method used) and subsequently be subject to a predetermined policy. Table 2 summarizes the benefits derived from the Cisco method as compared to competitive alternatives.

**Table 2.** Cisco Solution for Any Device Access: Features and Benefits

| Feature                              | Cisco | Others | Cisco Benefits   |
|--------------------------------------|-------|--------|--|
| <b>Scalable</b>                      | √     | ×      | Device profiling (fingerprinting) is very scalable because it does not happen at the controller, but rather at the Cisco Identity Services Engine (ISE). The controller is not burdened with yet another service.<br>Competitors using the wireless controller for fingerprinting significantly diminish performance by as much as 60 percent from theoretical throughput based on testing.  |
| <b>Multi-variable Fingerprinting</b> | √     | ×      | Instead of using a single profiling parameter (such as the device's browser) that can very easily be spoofed into pretending to be something that is not, Cisco uses more than five criteria, including: Netflow, MAC address, hostname, Dynamic Host Configuration Protocol (DHCP), and HTTP. By keeping the browser type at the end of the process, the Cisco methodology is able to eliminate virtually all false positives and avoid giving full network access to unmanaged devices (assuming that this is the desired policy). |
| <b>No RF Overhead</b>                | √     | ×      | Once a device is profiled, it can be placed onto the appropriate VLAN with the right policy controls. Competitive alternatives require the additional step of associating to a separate Secure Set Identifier (SSID), which can potentially slow down the network.   |
| <b>Rapid Profiling</b>               | √     | ×      | Cisco ISE keeps the device profile in a cache so that the process can be near instantaneous the next time it appears on the network. Controller-based solutions don't have the scalability to cache the information, and as a result perform repetitive tasks that further reduce performance.   |
| <b>Granular Policy Control</b>       | √     | √      | The Cisco ISE has the ability to manage very granular and fully customizable access policy levels that include up to four QoS categories, and a wide range of customizable access control lists (ACLs) and VLANs.  |

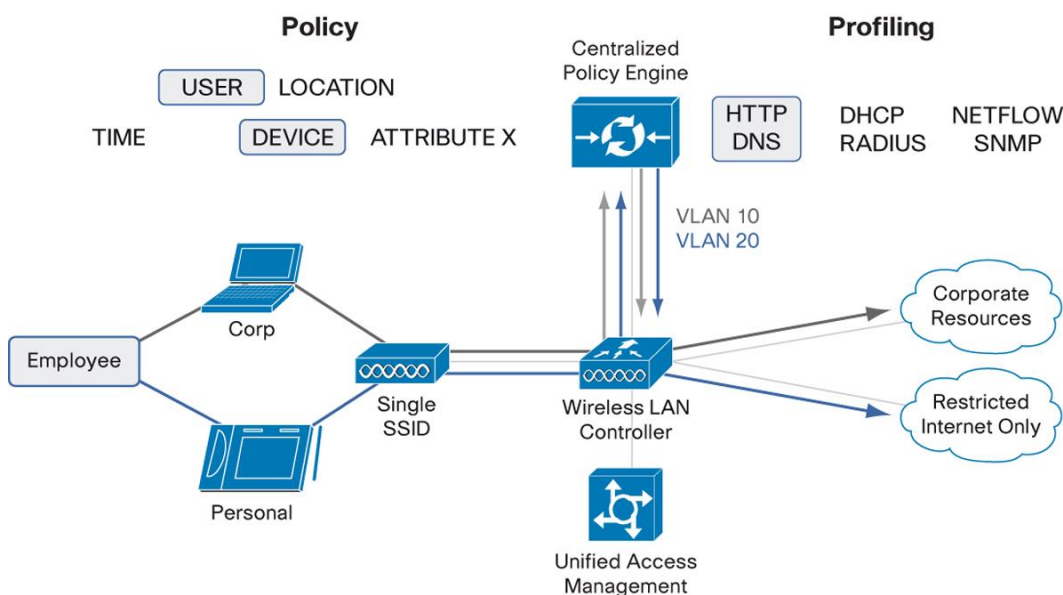
| Feature                      | Cisco | Others | Cisco Benefits   |
|------------------------------|-------|--------|--|
| <b>Integrated Posture</b>    | ✓     | ✗      | Posture assessment is an integral part of maintaining a secure enterprise network. The Cisco ISE integrates this functionality for a complete solution, whereas alternatives from competitors require a separate appliance that raises the cost of ownership.  |
| <b>Embedded Guest Access</b> | ✓     | ✗      | Finally, the Cisco ISE can also manage guest access, all from the same appliance, in order to significantly simplify network deployment and management. Most importantly, however, it does so for both wired and wireless clients. This is crucial because tablets are not the only unmanaged devices attaching to your network. |

Figure 2 illustrates the Cisco solution for any device access. Here is how it works:

- Employee brings both a corporate issued laptop and a personal tablet into the office.
- The employee connects both devices to the network using a single service set identifier (SSID). The network uses 802.1x Extensible Authentication Protocol (EAP) authentication.
- The Cisco ISE uses a number of device fingerprinting variables to accurately identify the device as a corporate or personal asset.
- An appropriate policy is determined using a combination of criteria such as who the user is, what device is being used, the location and time, and so on.
- The Cisco ISE then enforces the policy by placing each device on an appropriate VLAN while the device remains connected on the same SSID.
- The Cisco Wireless LAN Controller grants access to resources as appropriate based on policy. In the example shown in Figure 2, the corporate asset (laptop) gets unrestricted access to corporate resources, whereas the tablet is given restricted access as well as limited Internet access.

The Wireless LAN Controller grants access to resources as appropriate based on policy. In our example below the corporate asset (laptop) gets unrestricted access to corporate resources, whereas the tablet is given restricted access and limited to Internet access.

**Figure 2.** Cisco Solution for Any Device Access



---

## The Bottom Line

By now it should be evident that the influx of tablets and other unmanaged devices in the enterprise create a complex set of problems; these problems can't holistically be addressed without an architectural approach. Competitive solutions are primarily point solutions for wireless only and ignore most other challenges outlined in this paper. The Cisco Borderless Networks solution we've presented addresses role-based access for wired, wireless, and VPN, while performing device fingerprinting out of band. It also addresses critical security concerns such as what happens when a device is infected with viruses, when the device is lost or stolen and corporate data is compromised, or when the device is upgraded.

Additionally, Cisco holistically addresses the needs of enterprise mobile users by providing best-in-class RF tools that significantly improve the user experience.

A diligent comparison of the competitive alternatives will most certainly point out that "good enough" competitive solutions don't begin to compare with the Cisco solution, and that in the long run, higher operating expenses will far outweigh any capital savings achieved early on. The Cisco Borderless Networks solution for tablets will reduce your total cost of ownership in the following categories:

- **Fewer boxes to manage:** The Cisco ISE combines all the functionality required to get tablets (and all other devices) safely onto the network. You don't need to manage separate appliances for device fingerprinting, posture assessment, policy management, and guest access.
- **Single management platform:** Access is not wired or wireless - it is unified. You need a single-pane view of your wired and wireless network, and only Cisco can provide that capability. Cisco Prime NCS saves you money in deployment, training, troubleshooting, and maintenance of your network for years to come.
- **Better wireless network performance:** Cisco CleanAir, ClientLink, and VideoStream provide the best-in-class in RF technology, protecting the performance of your 802.11n network and optimizing the user experience and utility derived from tablets and other mobile devices.



---

**Americas Headquarters**  
Cisco Systems, Inc.  
San Jose, CA

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

**Europe Headquarters**  
Cisco Systems International BV Amsterdam,  
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at [www.cisco.com/go/offices](http://www.cisco.com/go/offices).

Cisco and the Cisco Logo are trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and other countries. A listing of Cisco's trademarks can be found at [www.cisco.com/go/trademarks](http://www.cisco.com/go/trademarks). Third party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1005R)