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

Mobile 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, as more and more users depend on tablets, such as the Apple iPad, for a variety of daily personal and professional tasks.

Tablet Computer Trends

Three main trends are emerging in the way enterprises handle the influx of these devices. First, Forrester attributes 30 percent of tablet purchases to companies providing tablets to their employees as their primary computing device. Some of these companies go as far as developing custom applications that solve key business problems. Second, several companies seek to improve employee satisfaction by allowing their employees to choose what type of mobile device they prefer instead of forcing them into an already set menu of choices. Finally, many companies are essentially ignoring the issues raised by the popularity of these devices. In doing so, they may be putting their networks at risk by not instituting controls on how these devices access network resources. Or if they simply prohibit the use of these devices, they put employee satisfaction at risk.

The Challenges

The influx of tablets in the enterprise brings a variety of challenges that IT departments need to address:

User Experience and Utility Challenges

Companies that sponsor or embrace tablets seek to maximize ROI and employee productivity. End-user experience and the usefulness of these devices depends on the network's ability to deliver interactive multimedia experiences and to support tablets in taking advantage of network intelligence, so that custom applications that increase operational efficiency can be built.

Additionally, the quality of user experience depends on bandwidth availability and careful network design, particularly when virtual desktop applications put a lot of pressure on networks during "bursting" intervals and also when these clients roam between access points.

Security Challenges

Getting unmanaged devices on the network and ensuring data integrity once they leave the network can be one of the biggest challenges IT will have to solve with tablets. Unmanaged devices are inherently risky and should be carefully screened for the right security updates and patch levels before they are allowed onto the network. Once authenticated, these devices need to be assigned a policy to determine the level of access that the device is granted. Policy is typically determined by such variables as who the user is (role in the organization), what device is being used, where and when access is permitted. Furthermore, IT needs to consider how to protect the device from connecting to an unsecured network, or how to handle sensitive data when family or friends use this noncorporate asset. Finally, a multilayered security approach is needed to protect users against infected websites and port 80 malicious traffic.

Manageability Challenges

IT departments are seeing their resources being quickly drained by the increasing need to manage and troubleshoot devices. In some cases, these activities may consume up to 30 percent of the IT budget. The influx of tablets in the enterprise also creates a network-planning nightmare for many organizations. To create an actionable capacity plan, it's vital to have a historical point of view into the types of devices in your network, their relative growth, and the demands they place on network resources. Finally, to effectively manage a network, you need to include all device and user combinations, including guest users.

The Cisco Solution

Cisco® Borderless Networks is the architectural approach required to meet all the challenges outlined above. The solution is founded on Cisco's best-in-class wireless networking and security solutions. These solutions deliver a unified approach to dealing with wired and wireless clients entering the enterprise.

The Cisco Unified Wireless Network supports interactive multimedia experiences on tablets by enabling reliable multicast over wireless with Cisco VideoStream technology, while the Cisco Compatible Extensions program ensures compatibility with over 90 percent of wireless devices. Cisco context-aware software exposes network intelligence, such as location, to third-party partners through an open API. As a result, tablet computers become more useful because they can run intelligent applications. In addition, Cisco innovations improve the performance of tablets in the following ways:

- Cisco CleanAir technology protects 802.11n performance by mitigating wireless interference
- Cisco ClientLink technology improves legacy 802.11a/g throughput by up to 65 percent
- The Cisco BandSelect feature optimizes radio load by pushing dual-radio clients to the less crowded 5-GHz frequency

In addition, Cisco Prime Network Control System (NCS) provides unified visibility into the converged wired and wireless access network, significantly reducing deployment and management costs associated with device troubleshooting.

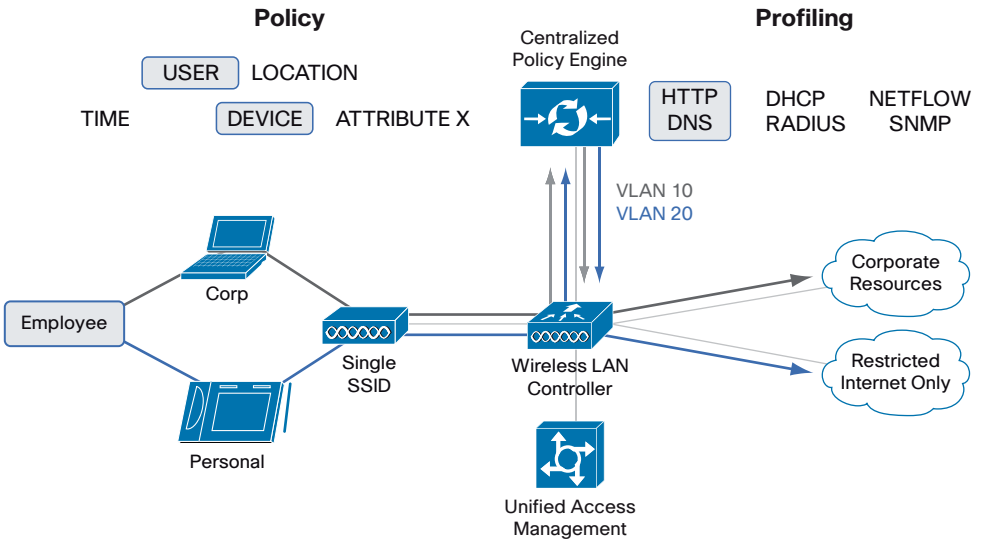
Cisco security solutions make getting these devices on the network easy. The Cisco Identity Services Engine (ISE) is a single appliance that profiles devices, assesses their posture, and enforces both wired or wireless

access policy. Additionally, it integrates guest access functionality, empowering employees to sponsor visitor access in a simplified interface with complete auditing and accountability of the guest. Cisco AnyConnect™ Secure Mobility protects device connections all the time by automatically creating a secure tunnel (VPN) through any Wi-Fi connection when off-premises. It also protects mobile users from web-based threats and enforces consistent web security policy using the premises-based Cisco IronPort™ Web Security Appliances or Cisco ScanSafe Cloud Web Security. Finally, Cisco Security Intelligence Operations (SIO) provides real-time global threat visibility and automatic protection to Cisco security deployments.

The most prevalent use case that IT departments need to solve for is the one where an employee brings their own personal device into the company and seeks to gain network access. Figure 1 illustrates the Cisco solution. 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.

Figure 1. Cisco Solution for Any Device Access



In the example shown in Figure 1, the corporate asset (laptop) gets unrestricted access to corporate resources, whereas the tablet is given restricted access as well as limited Internet access.

The Bottom Line

The influx of tablets and other mobile devices in the enterprise poses one of the biggest challenges IT is called to solve for. The Cisco Borderless Networks solution for tablets is one of the industry's most:

- Scalable: Uses the Cisco Identity Services Engine instead of a controller
- Accurate: Uses multi-variable fingerprinting
- Lean: Does not create RF overhead with multiple SSIDs
- Fast: Reduces reauthentication time through the use of a cache
- Granular: Offers fully customizable policy levels

Furthermore, the Cisco Borderless Networks solution for tablets reduces your total cost of ownership by:

- Requiring fewer boxes to manage: The Cisco Identity Services Engine combines all the functionality required to get tablets (and all other devices) safely onto the network, including posture assessment and guest access.
- Providing a single management platform: Access is not wired or wireless, it is unified. You get a single pane view of your wired and wireless network.
- Protecting wireless network performance: Cisco CleanAir, ClientLink, VideoStream, and BandSelect technologies provide the best-in-class RF solutions to protect the performance of your 802.11n network and optimize the user experience.

C45-674188-00 06/11