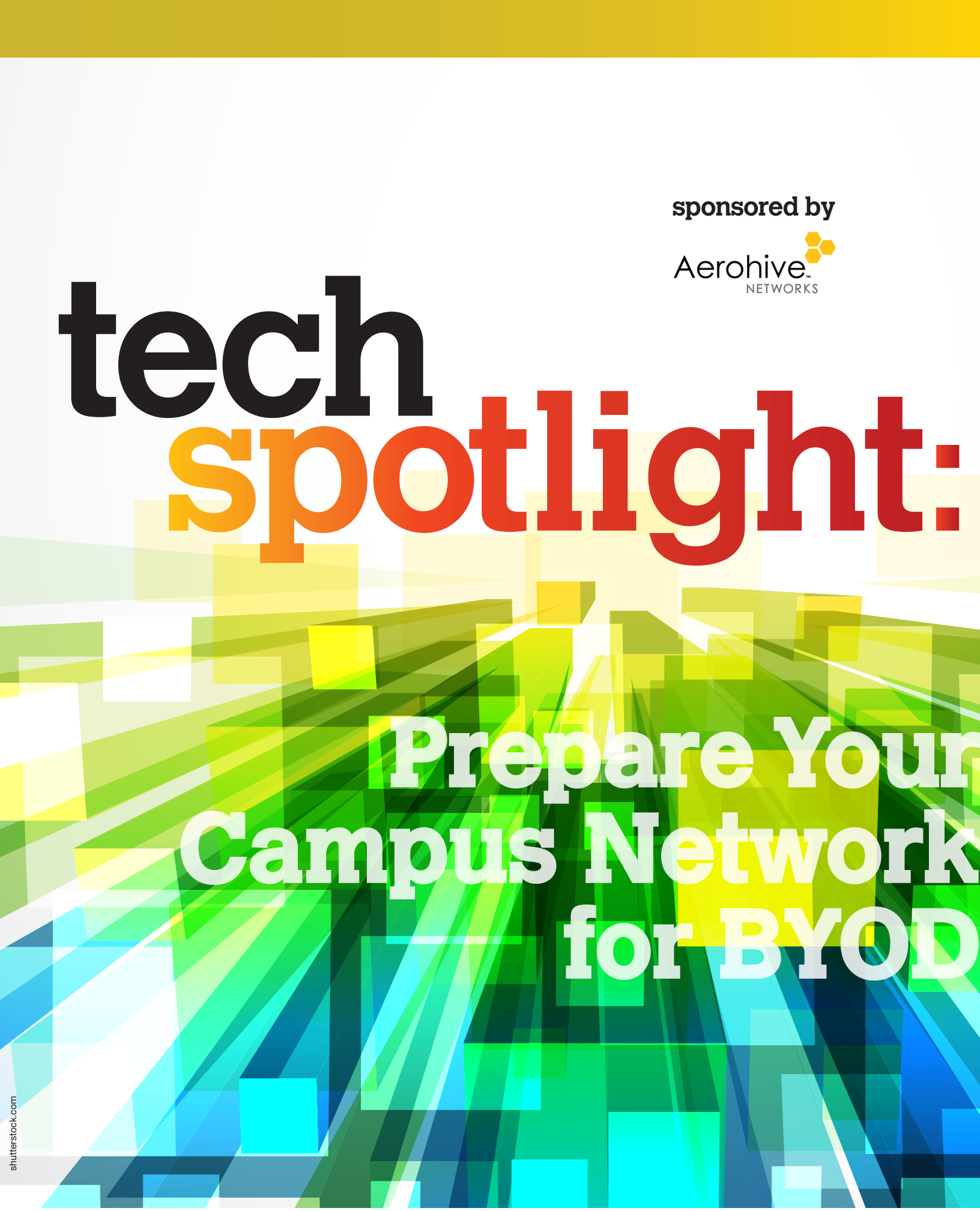
sponsored by

Aerohive NETWORKS

tech spotlight:

Prepare Your Campus Network for BYOD



shutterstock.com

Presented by Campus Technology

1105 MEDIA Education Group

TABLE OF CONTENTS

Sponsored by:

Aerohive NETWORKS

Presented by:

CAMPUS TECHNOLOGY

Smart Connected Devices Hit Record Levels Even as PCs Decline

BY DAVID NAGEL

In the last year, both desktop and portable PCs experienced declines in both mature and emerging markets worldwide. Meanwhile, smart phones and tablets carried the "smart connected device" category to new highs, topping 1 billion units worldwide, according to a new report released this week by market research firm IDC.

Worldwide Outlook

Smart connected devices include desktop PCs, laptops, tablets, and smart phones. IDC tracks worldwide shipments of these devices by unit and dollar value. For the year 2012, the total number of smart connected devices shipped worldwide hit 1.2 billion units for a total value of $576.9 billion. Overall worldwide growth was 29.1 percent.

According to IDC, tablets alone jumped 78.4 percent from 2011 to 2012, reaching 128 million devices. Smart phones reached 722.4 million units. Portable PCs and desktop PCs fell to 202 million and 148.4 million, respectively.

"Going forward, IDC expects that tablet shipments will surpass desktop PCs in 2013 and portable PCs in 2014, according to IDC. "In 2013, worldwide desktop PC shipments are expected to drop by 4.3 percent and portable PCs to maintain a flat growth of 0.9 percent. The tablet market, on the other hand, is expected to reach a new high of 190 million shipment units with year-on-year growth of 48.7 percent while the smartphone market is expected to grow 27.2 percent to 918.5 million units."

Overall worldwide growth in smart connected devices is expected to be 21.2 percent in 2013 and 8.5 percent by 2017, with tablets and smart phones continuing to drive growth.

In the fourth quarter specifically, IDC noted, a total of 378 million smart connected devices shipped, with revenues hitting more than $168 billion. In the same period according to IDC, Apple and Samsung led in shipments and dollar volume: "In terms of market share, Apple significantly closed the gap with market leader Samsung in the quarter, as the combination of Apple's iPhone 5 and iPad Mini brought Apple up to 20.3 percent unit shipment share versus 21.2 percent for Samsung. On a revenue basis for the fourth quarter, Apple continued to dominate with 30.7 percent share versus 20.4 percent share for Samsung.

Regional Variations: Mature Markets

In both emerging and mature markets, portable and desktop PCs saw declines, though portable PCs are expected to rebound a bit this year in emerging markets.

In 2012, in mature markets like the United States and Japan, overall growth in smart connected devices was 15.6 percent in 2012, with 2013 forecast at a growth rate of 13.8 percent.

Desktop PCs fell 4.8 percent from 2011; portable PCs fell 8.1 percent. This year, the declines will continue in mature markets, with desktops expected to shed another 5.5 percent off 2012's shipments and portables expected to lose 3.1 percent. Looking further out, desktops will drop another 2.9 percent by 2017, with portables falling off another 1.4 percent.

Meanwhile, tablets saw year-over-year growth of 62.8 percent in 2012. IDC predicted

Smart Connected Devices Hit Record Levels Even as PCs Decline
(continued)

that growth would slow to to 41.4 percent in 2013 and to 8.3 percent in 2017.

Smart phone shipments in mature markets grew 20.6 percent in 2012. IDC predicted growth will slow to 15.1 percent in 2013 and 4.6 percent by 2017.

Growth in Emerging Markets

In emerging markets, desktops fell off 3.8 percent in 2012 and will lose another 3.5 percent in 2013, though according to IDC that will be the last decline for desktops in emerging markets through 2017. Portable PCs fell a scant 0.8 percent in 2012. By next year, IDC predicted, portables will rise 4.1 percent in units shipped and another 7.1 percent by 2017.

Tablets, however, saw triple-digit growth from 2011 to 2012 in emerging markets, hitting 111.3 percent. IDC indicated that growth would slow in 2013, at 60.7 percent, and hit the low double digits by 2017 (13.4 percent).

Smart phones grew 69.7 percent in emerging markets in 2012 and will also see some slowdown in the coming years: 35.1 percent in 2013 and 12.2 percent by 2017.

Overall, shipments of smart connected devices grew 41.3 percent in 2012 in emerging markets. This year, IDC predicted, that growth would slow to 26.6 percent and slow further to 10.9 percent by 2017.

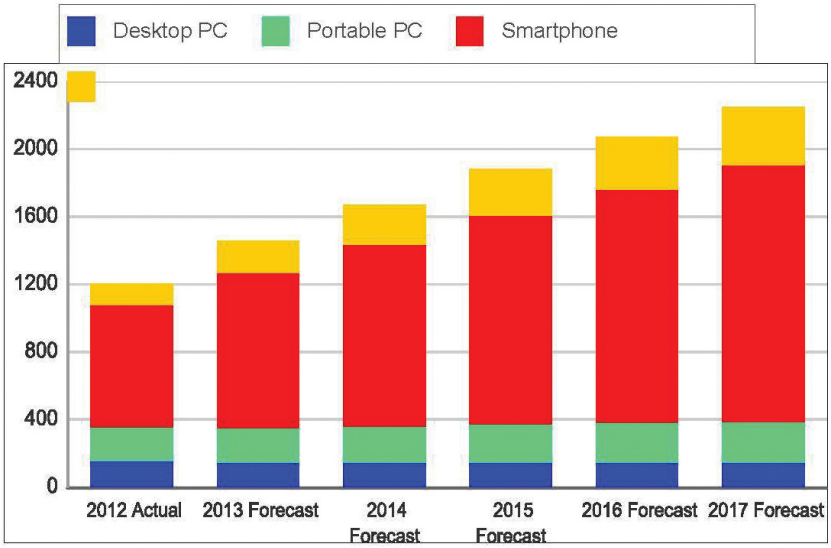
"In emerging markets, consumer spending typically starts with mobile phones and, in many cases, moves to tablets before PCs," said Megha Saini, research analyst for IDC's Worldwide Smart Connected Device Tracker, ina prepared statement. "The pressure on the PC market is significantly increasing and we can see longer replacement cycles coming into effect very soon and that, too, will put downward pressure on PC sales."

"Consumers and business buyers are now starting to see smartphones, tablets, and PCs as a single continuum of connected devices separated primarily by screen size," added Bob O'Donnell, IDC Program vice president for clients and displays. "Each of these devices is primarily used for data applications and different individuals choose different sets of screen sizes in order to fit their unique needs. These kinds of developments are creating exciting new opportunities that will continue to drive the smart connected devices market forward in a positive way."

The complete report, Smart Connected Device Tracker, can be accessed on IDC's site.

IDC
Analyze the Future

Worldwide Smart Connected Devices Market Forecast
Unit Shipments (Millions), 4Q 2012



About the Author

David Nagel *is the executive producer for 1105 Media's online K-12 and higher education publications and electronic newsletters. He can be reached at dnagel@1105media.com. He can now be followed on Twitter at http://twitter.com/THEJournalDave (K-12) or http://twitter.com/CampusTechDave (higher education). You can also connect with him on LinkedIn at http://www.linkedin.com/profile/view?id=10390192.*

Copyright © 2013, 1105 Media Inc.
For private use only, please visit
www.1105reprints.com
for licensing/reprint information.

The New Varsity Letters: BYOD = NAC + MDM

BY TONI FUHRMAN

To protect sensitive data in the BYOD era, schools must take a more closed, corporate approach, blending network access control and mobile device management.

By its very nature, education is "open." In contrast to the corporate world, schools provide access to a wide range of information—to a wide range of people. But, for better or worse, times are changing. For many network administrators in higher ed, open access has become a hornet's nest, and the era of limited lockdown has begun. And, increasingly, schools are looking to the business world for models on how to protect themselves and their constituents.

A case in point is New York Law School. Until the smartphone craze picked up, the school supported about 3,000 devices for its 1,500 students and 200-plus faculty. That figure jumped rapidly to 7,000 devices—mostly wireless—forcing Peter Trimarchi, NYLS's technical director, to take a hard look at the vulnerability of his network and its attendant devices.

"Over the last six months to a year, NYLS has been looking at this as a security issue," explained Trimarchi. "From a holistic security approach, we're monitoring computers. So we had to ask ourselves why we were not also doing this for mobile devices? Why weren't we securing our network completely?" Other issues loomed, too, such as how to deal with lost or stolen devices, how to make sure sensitive content doesn't fall into the wrong hands, and what to do about devices that become infected.

As a first step, Trimarchi and his team initiated a mobile device management (MDM) pilot that will continue through the summer, after which it will be "married" with a budget. The new system should be in place by next fall.

NYLS is considering a number of MDM products from different vendors. The school plans to use its existing network access control (NAC) appliance as the foundation for its security strategy, combined with MDM to secure data on BYOD devices. Paired together, the school should be able to manage everything on its network with unified visibility and control.

"The NAC appliance handles—but is not limited to—our web authentication, and our internal device wired and wireless security policies," explained Trimarchi. "MDM, on the other hand, is focused around mobile devices."

MDM Requirements

Among the features that NYLS requires of any MDM solution is the ability to authenticate devices, to track where they are on the network, to "wipe" them if they're lost or stolen, and to distinguish between what belongs to the university and what is personal. "If it's a user's own device, we want to wipe only what's corporate, while leaving personal data intact," noted Trimarchi. This is especially important for devices belonging to faculty, who often have access to shared drives and specific application needs. "We want faculty to be able to access things—to map network drives to devices—but we also want to protect them."

On the faculty side of device management, other important requirements include password policies, the ability to remotely locate devices and to detect jailbroken or rooted devices (which allow the device to install and run third-party applications). In addition, Trimarchi wants the ability to block personally identifiable information, track data usage for expense management, and get inventory reports. To reduce pressure on IT support staff, he also wants a self-service portal where users can reset their own passwords.

For students, the requirements are slightly different. Students will be able to authenticate via an active directory, enabling them to connect to the e-mail system. A physical help desk will also be available to assist students with issues.

Given how lax students can be when it comes to software updates, peer-to-peer file sharing, and antivirus software, the ability to quarantine mobile devices that don't adhere to school standards is a critical component of any MDM solution. "By next fall, we're hoping that students will be able to authenticate each of their devices and be subject to the policies we put in place," continued Trimarchi. "If a phone is hacked or has a virus, for instance, we can block it or quarantine it, and we can assist the student in cleaning up the device."

The change from the educational ideal of open information to a more closed, corporate approach is a "huge thing," according to Trimarchi. "With a virtual private network, you get whatever the machine throws out. But, with products like ForeScout, you have to meet certain requirements. If you don't adhere to the policy, you don't get on the network."

Getting Started

For schools considering a similar, holistic approach to security, Trimarchi advises schools to "look at what's out there and try it out. Kick the tires on all vendors." As part of the due diligence process, he recommends that IT shops check blogs and ask questions about vendors in technical forums. And when it comes to a contract, make sure that the company is committed to everything it says it can do.

Regardless of which vendor a school chooses, though, it shouldn't expect a fire-and-forget solution. Once the new policies are in place at NYLS, for example, Trimarchi estimates a six-month adjustment period. "People will come to me with ideas," he predicted. "We'll make adjustments. We'll be tweaking it."

He noted that, even now, Samsung is making a watch that will be able to get on the network. "We can't get ahead," said Trimarchi ruefully. "We're always behind."

About the Author

Toni Fuhrman is a writer and creative consultant based in Los Angeles.

Copyright © 2013, 1105 Media Inc.
For private use only, please visit www.1105reprints.com for licensing/reprint information.

Aerohive NETWORKS

case study

Tennessee Tech University

Tennessee Tech University Extends Reliable, Centrally Managed WLAN throughout its Sprawling Campus with Aerohive

Challenges

- Tennessee Tech University needed an easy to deploy, cost-effective enterprise-class wireless network.
- With so many types of devices on a university campus, the Information Technology Services department was confronted with device management complexities, including BYOD.
- The university also needed a wireless LAN that would integrate with the existing network infrastructure for a simple migration that was easy to manage and would scale cost-effectively across the campus.

Results

- Applications with high-performance connectivity have increased students' and professors' productivity in the classroom.
- A resilient wireless network created a secure learning environment that maintained access for visitors.
- The network was easy for ITS to manage, monitor and control from a central location, which gave its staff more time to do their work without traveling across the campus.

About Tennessee Tech University

The state's only public technological university, Tennessee Tech University (TTU) is nationally ranked and offers more than 40 undergraduate and 20 graduate programs across six academic divisions. The university consists of 87 buildings on more than 200 acres and enrolls more than 11,700 students.

The university is governed by the Tennessee Board of Regents. Founded in 1915, it is approximately an hour east of Nashville in Cookeville, Tenn.

> "As the environment changes, we have to adapt to it. That's one of the nice things about Aerohive; we're not concerned at all about controllers, which limit how quickly we can grow a network."
>
> **—Jerry Boyd**
>
> Director of Network Services and Operations, Tennessee Tech University

The Problem

Like most universities and organizations, TTU needs to stretch its budget and make its investments matter.

Jerry Boyd, director of network services and operations for TTU, was well aware of this as he assessed the aging network infrastructure upon which the university's students, teachers and community relied.

"As the environment changes, we have to adapt to it," Boyd said. "That's one of the nice things about Aerohive; we're not concerned at all about controllers, which limit how quickly we can grow a network."

With the Aerohive system, ITS will be able to add more access points as the university grows and demand increases.

The Results and Benefits

Boyd said Aerohive's Bonjour Gateway is one of the features he is looking forward to using the most because of the high number of Apple products on campus.

Aerohive's Bonjour Gateway makes Apple services such as AirPrint, AirPlay and remote display with Apple TV usable across large networks.

The capabilities that Bonjour enables are very attractive to enterprises and educational institutions for their ease of use and ability to help make BYOD initiatives more productive. And Aerohive's patent-pending Bonjour Gateway is designed to vastly simplify the support of Apple compatible devices at universities.

With Aerohive BR100 Routers, administrators set up one configuration for remote devices via the HiveManager interface; when the BR100 is plugged in, it discovers the HiveManager automatically.

The BR100 enables administrators to run a thousand remote office VPNs as easily as a single location. In addition to 802.11n WiFi, the BR100 supports multiple SSIDs and VLANs shared across wired and wireless interfaces, which can be configured in a number of ways to handle any small office/teleworker requirements.

"We're looking at those for the VPN-type access — people working from home or people who are traveling and need a secure solution to get back into (the network)," Boyd said.

Those who travel and need BR100s include university administrators, the ITS team and athletic recruiters.

Tennessee Tech's classrooms have mobile online learning environments, which allow students to log in to a virtual desktop using any device. The environment supports the BYOD reality and Aerohive plays a key role in the system.

TTU began implementing the Aerohive network in the spring of 2011.

Aerohive NETWORKS

Contact us today to learn how your organization can benefit from Aerohive wireless LAN architecture.

Aerohive Networks, Inc.
330 Gibraltar Drive
Sunnyvale, CA 94089

toll free 1-866-918-9918
phone 408-510-6100
fax 408-510-6199

www.aerohive.com
info@aerohive.com
CS-Tennesse Tech_1212

Aerohive NETWORKS

solution brief

Bonjour Gateway

Table of Contents

Copyright ©2012, Aerohive Networks, Inc.

Enterprise-level "Zero-Configuration Networking" for Apple Devices

Bring Your Own Device (BYOD) and the consumerization of IT may be overused as market terms but they are unquestionably a trend that is changing network architectures in almost every enterprise. In a recent survey by Dimensional Research of 750 front-line IT professionals, managers, and executives, 87% say that today their employees already use personal devices for work-related activities. These results are verified by more and more surveys across different verticals every day. These devices, 80% of which are identified as smart mobile devices, are simplified for ease of use and therefore enhance employee productivity. However, for the IT department, it means a shift in network intelligence and capability out of the device and puts more onus onto the network infrastructure.

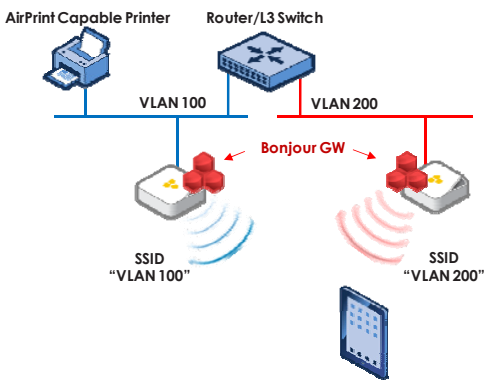
Aerohive has developed the industry's most intelligent edge architecture and built it from the ground up for the shift to smart mobile devices (smart phones, tablets, and mobile laptops) as the primary access device and the consumerization of IT (corporate-owned consumer devices). Cloud-enabled networks with distributed intelligence provide inherent network-based mobile device management, corral the "iEverything" BYOD explosion, and simplify the very complex enterprise network problem of how to deal with high-speed mobile smart devices.

There are many challenges with the BYOD trend but one of the key attributes that makes a network purpose-built for mobility and operationally simple for BYOD and the consumerization of IT is the ability to create "Zero-Configuration Networking" available to large organizations and enterprises so that consumer devices work on the enterprise network with no end user expertise. In order to fully realize this concept the network infrastructure must become "service-aware" and simply provide service availability seamlessly across the network and control access to those services based on a users' context – identity, location, application, and device in use. In a service-aware network, an authorized user should instantly see services available to them such as printers, video projection, and collaboration applications, without configuring their smart mobile device. This is the ultimate achievement in the attempt to make BYOD not just manageable as an IT initiative, but desirable as it makes the BYOD user both less expensive from a capital expenditure (as the employee has purchased the device) and from an operational expense as policy and service availability is set by user context and automatically connected to the end device.

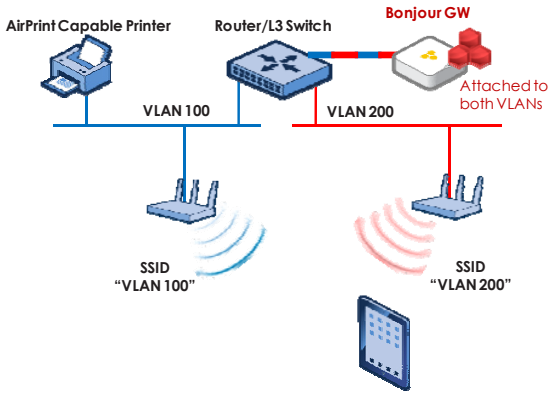
Aerohive has a history of defining the future of networking and is once again paving the way with the introduction of the first service aware infrastructure technology. 72% of the devices brought into the enterprise by users are Apple devices, according to Dynamic Research, and as such Aerohive has introduced native Bonjour awareness and control into our Cooperative Control architecture to support Apple's "Zero-Configuration Networking" for products in the enterprise and larger educational institutions.
To make networks service-aware and make BYOD with Apple devices a native part of every network, Aerohive has built a Bonjour Gateway to manage and control Apple service availability (such as AirPrint™, AirPlay®, file sharing, collaboration applications, etc.) across an entire enterprise network. This patent-pending functionality is a native part of Aerohive's HiveOS network operating system and as such even non-Aerohive legacy networks can manage their services by attaching a single Aerohive device, via a trunk port, to the network – the gateway functionality works out-of-band. Managing Apple services across an enterprise network is now extraordinarily simple: If a service,

Copyright ©2012, Aerohive Networks, Inc.

such as a printer, announces itself, Aerohive can ensure that the printer advertisement is made available across the entire network or, if necessary, make sure it's available only to the networks allowed to view the service (i.e. control the service advertisements).



Bonjour Gateway in an Aerohive network



Bonjour Gateway in a legacy non-Aerohive network

Bonjour Gateway and Apple's Bonjour Protocol

Bonjour underlies many services that are widely used on Apple-centric networks. By monitoring Bonjour advertisements, clients can learn the location (IP address and port) of any service, and then connect to it as with any other service. Bonjour transforms the manual process of configuring IP addresses and port numbers into a "plug-and-play" experience where users reference services by type and a human-readable name. Two notable examples are AirPrint and AirPlay. Both advertise themselves through Bonjour to enable clients to print and display screens, respectively. AirPlay is especially valuable in many contexts for remote display from iOS devices, and the recent announcement that AirPlay will be available in the next version of Mac OS® (code-named Mountain Lion) only makes it more compelling.

The capabilities that Bonjour enables are very attractive to enterprises and educational institutions for their ease of use and ability to help make BYOD initiatives more productive (where IT doesn't have to install all the services on every device – even the ones it doesn't own). The problem comes in when one tries to scale Bonjour from home applications to broad, multi-vendor, multi-segment networks. Because Bonjour relies on an underlying multicast DNS advertisement, it is restricted to the scope that that advertisement travels across the network. As an example, on a network that lacks the Aerohive Bonjour Gateway, AirPlay will only function when both the Apple TV and the display source are both attached to the same broadcast link. Client devices cannot use AirPlay unless they are attached to the same VLAN as the Apple TV. In many enterprise and education networks, this restriction is unattractive.

One of the key building blocks that Bonjour is built on is multicast DNS. Services send advertisements to a link-local IP address, and clients build a list of available services by listening to those advertisements. On networks that consist of a single broadcast domain, the use of link-local IP addressing is acceptable. Once a network is built with segmented broadcast domains for scalability, however, multicast DNS advertisements no longer reach all devices on the network. While many services will be local to the immediate network link, not all will be.

Copyright ©2012, Aerohive Networks, Inc.

As an example, consider the network in Figure 1. VLAN 100 on the left side of the provides multiple services. A printer advertises AirPrint capabilities through Bonjour, the Apple TV advertises AirPlay service, and the server provides file sharing. When the tablet is attached to the VLAN 100 Network SSID on the left-hand AP, it is able to use any services on that network. If it moves across the router by attaching to the VLAN 200 Network SSID, it will no longer receive multicast DNS advertisements for any of those services.

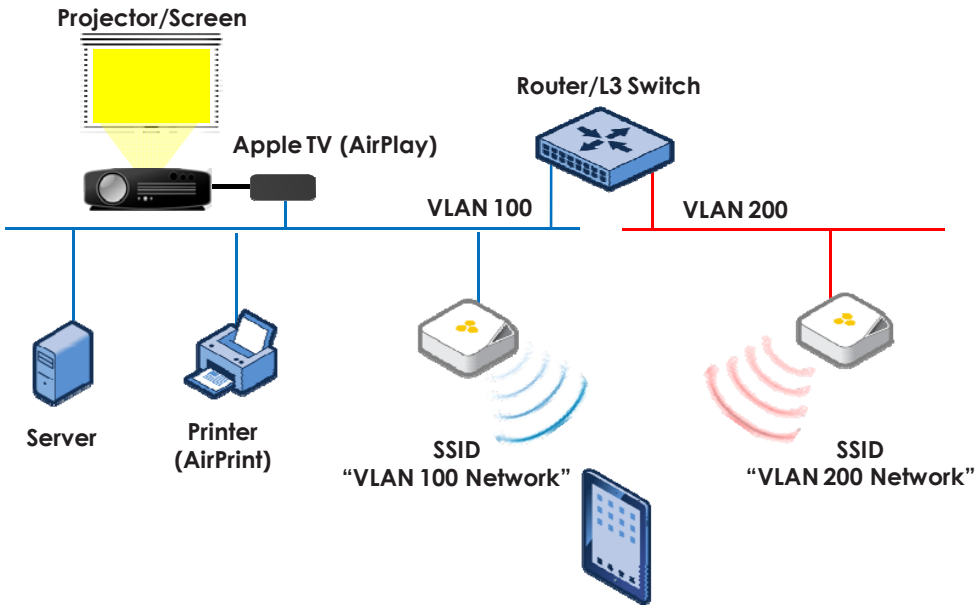


Figure 1: Example Multi-Subnet Network

Ensure Students are Connected – to the Right Content

When Aerohive first considered how to solve this problem, the first approach was a narrow solution to bring all devices together on to the same broadcast domain. Through Aerohive's layer-3 tunneling capabilities and private pre-shared key features, it would be possible to configure all Apple TVs throughout the network to attach to the same VLAN regardless of the underlying topology. However, most devices will need to use several services, so it is not generally possible to set up a VLAN for each service. If, for example, iPads® need to both print and use AirPlay, then all Apple TVs and all printers must be on the same VLAN. Taken to its extreme, the network becomes a single VLAN with all available services. Such a network concentrates all traffic through a set of "choke points" that lack scalability, redundancy, and sap the network of efficiency.

A second approach considered was to forward all multicast advertisements across router boundaries. Doing so would undoubtedly make services widely available, but forwarding link-local multicasts is explicitly forbidden by the router requirements RFC. Furthermore, many access network devices are constructed so that the core switch fabric forwards unicast packets, while multicast packets are either flooded to all ports or handled by the CPU outside of the switch fabric. Simply forwarding all multicast advertisements would cause an unacceptable load on the access network, both in

Copyright ©2012, Aerohive Networks, Inc.

terms of processing power on the access layer as well as on network capacity. Forwarding all multicast advertisement frames results in every service on the network being advertised on every VLAN. On a large network, not every service should be advertised network-wide. A corallary to this problem is that of advertising services from devices (printers, Apple TVs, file services, etc.) that are spread all across the enterprise or campus and span multiple VLANs. If this multicast methodology were used then there would be a "multicast direction" issue, in other words, you wouldn't want VLAN1 services to be sent out to all other VLANs and then VLAN2 sending the multicast back across the router boundary advertising its services in return as these "blind" multicast forward mechanisms run the danger of causing a loop and harming network and service performance.

How it All Comes Together

In designing the Bonjour Gateway technology, Aerohive combined the ease of use of multicast forwarding with awareness of the underlying advertisement protocols. In Figure 1, the access point on VLAN 100 receives advertisements from the printer, Apple TV, and server. Information on available services is then selectively relayed to the access point on VLAN 200. Services that are shared between the two networks are then re-advertised on VLAN 200, and can be detected by attached devices. If permitted by security policies installed and enforced between the two VLANs, any devices attached to the right-hand SSID are able to find, configure, and use any services learned from VLAN 100.

Figure 2: AirPlay in Use

When the gateway is activated, it enables the sharing of link-local service advertisements across the router boundary. Figure 3 shows an Apple iPad displaying the AirPlay service advertisement from an IP address on VLAN 100 (192.168.1.0/24) even though the iPad itself is attached to VLAN 200 (192.168.200.0/24).

Copyright ©2012, Aerohive Networks, Inc.

Bonjour Gateway

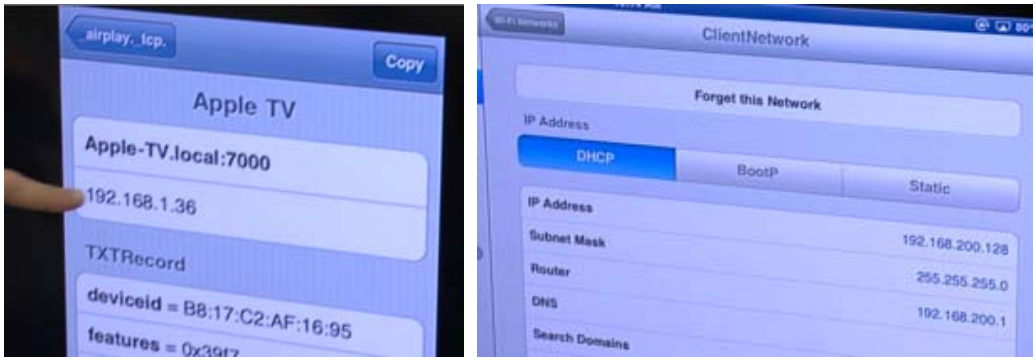


Figure 3: AirPlay Advertisement Crossing Subnet Boundary

Many networks support a large number of services, and on networks with significant numbers of Apple devices, it may be undesirable to share all services across all networks. Depending on the applications supported by the network, it is likely that only a few services must be supported network-wide. For example, it might be desirable to make printers available across a network regardless of the underlying topology. If Apple TVs are used in many conference rooms or classrooms simultaneously, it may be desirable to share only Apple TV services.

To prevent network overload, the Bonjour Gateway supports service filtering. Figure 4 shows the service list available on an iPad. In the left screen shot, the screen mirroring shows a long list of services advertised from computer on VLAN 100 in the network diagram. In the right screen shot, the iPad has moved to VLAN 200. However, the Bonjour Gateway has been configured to allow only AirPlay to pass across the router.

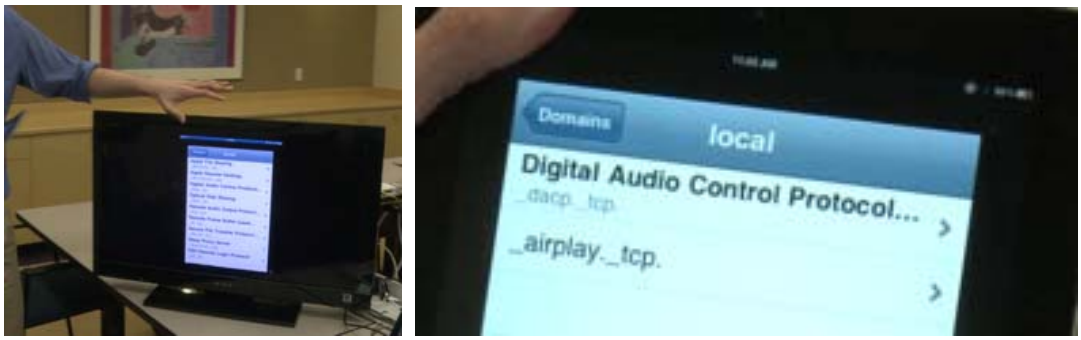


Figure 4: Filtering in Action

Copyright ©2012, Aerohive Networks, Inc.

Summary

Aerohive's patent-pending Bonjour Gateway capability takes service advertisements that are restricted to a single broadcast link and makes those services available network-wide, without any client modifications or networking gymnasitics.

Aerohive Bonjour Gateway Benefits

- Multi-Vendor - Works in both Aerohive and Non-Aerohive networks
- Plug and Play - No requirement for VLAN and Multicast gymnastics
- Flexible - Supports bi-directional service advertisements, without fear of multicast loops and flooding
- Efficient – Gateway functionality enables - granular control, ability to respond to service queries and limits communication to changes in service availability
- Secure and Scalable – Preserves enterprise security policy and data forwarding methodology

Copyright ©2012, Aerohive Networks, Inc.

About Aerohive

Aerohive Networks reduces the cost and complexity of today's networks with cloud-enabled, distributed Wi-Fi and routing solutions for enterprises and medium sized companies including branch offices and teleworkers. Aerohive's award-winning cooperative control Wi-Fi architecture, public or private cloud-enabled network management, routing and VPN solutions eliminate costly controllers and single points of failure. This gives its customers mission critical reliability with granular security and policy enforcement and the ability to start small and expand without limitations. Aerohive was founded in 2006 and is headquartered in Sunnyvale, Calif. The company's investors include Kleiner Perkins Caufield & Byers, Lightspeed Venture Partners, Northern Light Venture Capital and New Enterprise Associates, Inc. (NEA).

Corporate Headquarters
Aerohive Networks, Inc.
330 Gibraltar Drive
Sunnyvale, California 94089 USA
Phone: 408.510.6100
Toll Free: 1.866.918.9918
Fax: 408.510.6199
info@aerohive.com
www.aerohive.com

EMEA Headquarters
Aerohive Networks Europe LTD
Sequel House
The Hart
Surrey, UK GU9 7HW
+44 (0)1252 736590
Fax: +44 (0)1252711901

SB1202403

PLUG IN.
ROAM ON.
LISTEN UP.
AIM HIGH.

Education-optimized WiFi.
Enhance learning and boost productivity with an easy-to-use wireless solution that provides integrated classroom control.

Elasticity. Simplicity. User-Centricity.

Get started with your free evaluation at
aerohive.com/education

Hive on.

Aerohive NETWORKS

About Us

About Aerohive

Aerohive Networks reduces the cost and complexity of today's networks with cloudenabled, distributed Wi-Fi and routing solutions for enterprises and medium sized companies including branch offices and teleworkers. Aerohive's award-winning cooperative control Wi-Fi architecture, public or private cloud-enabled network management, routing and VPN solutions eliminate costly controllers and single points of failure. This gives its customers mission critical reliability with granular security and policy enforcement and the ability to start small and expand without limitations. Aerohive was founded in 2006 and is headquartered in Sunnyvale, Calif. The company's investors include Kleiner Perkins Caufield & Byers, Lightspeed Venture Partners, Northern Light Venture Capital and New Enterprise Associates, Inc. (NEA).

About Campus Technology

Campus Technology is a comprehensive resource that includes a monthly magazine, website, newsletters, webinars, online tools and in-person and virtual events—providing in-depth coverage on the technologies and implementations influencing colleges and universities across the nation. You'll discover valuable how-to content, best practices, industry trends, expert advice and insightful articles to help administrators, campus executives, technologists and educators plan, develop and successfully launch effective IT initiatives. Visit our booth to sign up/renew your FREE magazine or newsletter subscriptions and to set up your *CampusTechnology*.com online account to access the FREE resource tools exclusively found on our website.